3Com S7900E Family

Command Reference Guide

Release 6300 Series

S7910E

S7906E

S7906E-V

S7903E

S7903E-S

S7902E

Manual Version:
20090615-C-1.01
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 S7900E Family Command Reference Guide - Release 6300 Series is organized as follows:

Volume	Features			
01-Access Volume	Ethernet Interface	Link aggregation	Port Isolation	Service Loopback Group
	DLDP	Smart Link	LLDP	VLAN
	GVRP	QinQ	BPDU Tunnel	VLAN Mapping
	Ethernet OAM	Connectivity Fault Detection	EPON-OLT	MSTP
	RRPP	Mirroring		
02-IP Services Volume	IP Address	ARP	DHCP	DNS
	IP Performance	UDP Helper	URPF	IPv6 Basics
	Tunneling	sFlow		
03-IP Routing Volume	IP Routing Overview	Static Routing	RIP	OSPF
	IS-IS	BGP	IPv6 Static Routing	IPv6 RIPng
	IPv6 OSPFv3	IPv6 IS-IS	IPv6 BGP	Routing Policy
04-IP Multicast Volume	Multicast Routing and Forwarding	IGMP	PIM	MSDP
	MBGP	Multicast VPN	IGMP Snooping	Multicast VLAN
	IPv6 Multicast Routing and Forwarding	MLD	IPv6 PIM	IPv6 MBGP
	MLD Snooping	IPv6 Multicast VLAN		
05-MPLS Volume	MCE	MPLS Basics	MPLS L2VPN	MPLS L3VPN
06-QoS Volume	QoS			
07-Security Volume	AAA	802.1x	MAC Authentication	Portal
	Port Security	IP Source Guard	SSH2.0	ACL
08-System Volume	Login	Basic System Configuration	Device Management	File System Management
	SNMP	RMON	MAC Address Table Management	System Maintenance and Debugging
	Information Center	PoE	Track	NQA
	NTP	VRRP	HA	Hotfix

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
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

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

Convention	Description
	damage to equipment.
 Highlight	Means an action or information that needs special attention to ensure successful configuration or good performance.
 Note	Means a complementary description.
 Tip	Means techniques helpful for you to make configuration with ease.

Related Documentation

In addition to this manual, each 3Com S7900E Family documentation set includes the following:

Manual	Description
3Com S7900E Family Configuration Guide - Release 6300 Series	Describe how to configure your S7900E Switch using the supported protocols and CLI commands.
3Com S7900E Family Getting Started Guide	This guide provides all the information you need to install and use the 3Com S7900E 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.

1 Feature List

The S7900E series support abundant features and the related documents are divided into the volumes as listed in Table 1-1.

Table 1-1 Feature list

Volume	Features			
01-Access Volume	Ethernet Interface	Link aggregation	Port Isolation	Service Loopback Group
	DLDP	Smart Link	LLDP	VLAN
	GVRP	QinQ	BPDU Tunnel	VLAN Mapping
	Ethernet OAM	Connectivity Fault Detection	EPON-OLT	MSTP
	RRPP	Mirroring		
02-IP Services Volume	IP Address	ARP	DHCP	DNS
	IP Performance	UDP Helper	URPF	IPv6 Basics
	Tunneling	sFlow		
03-IP Routing Volume	IP Routing Overview	Static Routing	RIP	OSPF
	IS-IS	BGP	IPv6 Static Routing	IPv6 RIPng
	IPv6 OSPFv3	IPv6 IS-IS	IPv6 BGP	Routing Policy
04-IP Multicast Volume	Multicast Routing and Forwarding	IGMP	PIM	MSDP
	MBGP	Multicast VPN	IGMP Snooping	Multicast VLAN
	IPv6 Multicast Routing and Forwarding	MLD	IPv6 PIM	IPv6 MBGP
	MLD Snooping	IPv6 Multicast VLAN		
05-MPLS Volume	MCE	MPLS Basics	MPLS L2VPN	MPLS L3VPN
06-QoS Volume	QoS			
07-Security Volume	AAA	802.1x	MAC Authentication	Portal
	Port Security	IP Source Guard	SSH2.0	ACL

Volume	Features			
08-System Volume	Login	Basic System Configuration	Device Management	File System Management
	SNMP	RMON	MAC Address Table Management	System Maintenance and Debugging
	Information Center	PoE	Track	NQA
	NTP	VRRP	HA	Hotfix

2 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

Access Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The Access Volume is organized as follows:

Features	Description
Ethernet Interface	This document introduces the commands for: • Combo Port Configuration • Basic Ethernet Interface Configuration • Configuring Flow Control on an Ethernet Interface • Configuring the Suppression Time of Physical-Link-State Change on an Ethernet Interface • Configuring Loopback Testing on an Ethernet Interface • Configuring a Port Group • Configuring an Auto-negotiation Transmission Rate • Configuring Storm Suppression • Setting the Interval for Collecting Ethernet Interface Statistics • Enabling Forwarding of Jumbo Frames • Enabling Loopback Detection on an Ethernet Interface • Configuring the MDI Mode for an Ethernet Interface • Testing the Cable on an Ethernet Interface • Configuring the Storm Constrain Function on an Ethernet Interface
Link Aggregation	Link aggregation aggregates multiple physical Ethernet ports into one logical link. This document introduces the commands for: • Configuring a Static Aggregation Group • Configuring a Dynamic Aggregation Group • Configuring an Aggregate Interface
Port Isolation	The port isolation feature allows you to isolate different ports within the same VLAN. This document introduces the commands for the isolation group configuration.
Service Loopback Group	To increase service redirecting throughput, you can bundle multiple service loopback ports into a logical link, called a service loopback group. This document introduces the commands for the service loopback group configuration.

Features	Description
DLDP	In the use of fibers, link errors, namely unidirectional links, are likely to occur. DLDP is designed to detect such errors. This document introduces the commands for: • Enabling DLDP • Setting DLDP Mode • Setting the Interval for Sending Advertisement Packets • Setting the DelayDown Timer • Setting the Port Shutdown Mode • Configuring DLDP Authentication • Resetting DLDP State
Smart Link	Smart Link is a solution for active-standby link redundancy backup and rapid transition in dual-uplink networking. This document introduces the commands for: • Configuring a Smart Link Device • Configuring an Associated Device
LLDP	LLDP enables a device to maintain and manage its own and its immediate neighbor's device information, based on which the network management system detects and determines the conditions of the communications links. This document introduces the commands for: • Performing Basic LLDP Configuration • Configuring the Encapsulation Format for LLDPDUs • Configuring the Encapsulation Format of the Management Address • Configuring CDP Compatibility • Configuring LLDP Trapping
VLAN	Using the VLAN technology, you can partition a LAN into multiple logical LANs. This document introduces the commands for: • Configuration of Super VLAN • Configuration of Isolate-User-VLAN • Configuration of Voice VLAN
GVRP	GVRP is a GARP application. This document introduces the commands for: • GVRP configuration • GARP Timers configuration
QinQ	As defined in IEEE802.1Q, 12 bits are used to identify a VLAN ID, so a device can support a maximum of 4094 VLANs. The QinQ feature extends the VLAN space by allowing Ethernet frames to travel across the service provider network with double VLAN tags. This document introduces the commands for: • Configuring basic QinQ • Configuring Selective QinQ • Configuring the TPID Value in VLAN Tags • Configuring an Inner-Outer VLAN 802.1p Priority Mapping
BPDU Tunneling	BPDU tunneling enables transparently transmission of customer network BPDU frames over the service provider network. This document introduces the commands for: • Configuring BPDU Transparent Transmission • Configuring Destination Multicast MAC Address for BPDU Tunnel Frames

Features	Description
VLAN Mapping	The VLAN mapping feature maps CVLAN tags to SVLAN tags. This document introduces the commands for: • Configuring One-to-One VLAN Mapping • Configuring Many-to-One VLAN Mapping • Configuring One-to-Two VLAN Mapping • Configuring Two-to-Two VLAN Mapping
Ethernet OAM	Ethernet OAM is a tool monitoring Layer-2 link status. It helps network administrators manage their networks effectively. This document introduces the commands for: • Configuring Basic Ethernet OAM Functions • Configuring Link Monitoring • Enabling OAM Loopback Testing
Connectivity Fault Detection	Connectivity fault detection is an end-to-end, per-VLAN link-layer OAM mechanism for link connectivity detection, fault verification, and fault location. This document introduces the commands for: • Configuring CC on MEPs • Configuring LB on MEPs • Configuring LT on MEPs
EPON OLT	EPON is a Passive Optical Network (PON) that carries Ethernet frames encapsulated in 802.3 standards. It is a combination of the Ethernet technology and the PON technology. This document introduces the commands for: • OLT Configuration • ONU Remote Management Configuration • UNI Port Configuration • Alarm Configuration
MSTP	MSTP is used to eliminate loops in a LAN. It is compatible with STP and RSTP. This document introduces the commands for: • Configuring the Root Bridge • Configuring Leaf Nodes • Performing mCheck • Configuring Digest Snooping • Configuring No Agreement Check • Configuring Protection Functions
RRPP	RRPP is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes after a link is disconnected on the ring. This document introduces the commands for: • Configuring Master Node • Configuring Transit Node • Configuring Edge Node • Configuring Assistant Edge Node • Configuring Ring Group

Features	Description
Mirroring	Port mirroring copies packets passing through a port to another port connected with a monitoring device for packet analysis to help implement network monitoring and troubleshooting. Traffic mirroring is implemented by a QoS policy, which defines certain match criteria to match the packets to be mirrored and defines the action of mirroring such packets to the specified destination.This document introduces the commands for: • Local port mirroring configuration • Remote port mirroring configuration On the S7900E series switches, traffic mirroring is achieved mainly through QoS policies and remote port mirroring. For QoS policy configuration commands, refer to *QoS Commands* in the *QoS Volume*.

Table of Contents

1 Ethernet Interface Configuration Commands

Ethernet Interface Configuration Commands

broadcast-suppression

Syntax

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

undo broadcast-suppression

View

Layer 2 Ethernet interface view, port group view

Default Level

2: System level

Parameters

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

pps *max-pps*: Specifies the maximum number of broadcast packets that can be forwarded on the Ethernet interface(s) per second.

- For a 100-Mbps port, this value ranges from 1 to 148810 (in pps).
- For a 1-Gbps port, this value ranges from 1 to 1488100 (in pps).
- For a 10-Gbps port, this value ranges from 1 to 14881000 (in pps).

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 interface may not be the one that actually takes effect. To display the actual broadcast suppression threshold value on an Ethernet interface, 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 or keyword should be no smaller than 1, and the broadcast suppression threshold value is the one that actually takes effect on the Ethernet interface.

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 interface, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet interface, 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 interface 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.
- On an Ethernet port enabled with broadcast storm suppression ratio, this feature takes effect only in the inbound direction.

Examples

For Ethernet interface Ethernet 2/0/1, allow broadcast traffic equivalent to 20% of the total transmission capability of Ethernet 2/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 ethernet 2/0/1
[Sysname-port-group-manual-group1] group-member ethernet 2/0/2
[Sysname-port-group-manual-group1] broadcast-suppression 20
```

description

Syntax

description *text*

undo description

View

Ethernet 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 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, **Ethernet2/0/1 Interface** for example.

Related commands: **display interface**.

Examples

Configure the description string of interface Ethernet 2/0/1 as **lanswitch-interface**.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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
Loop0                UP        UP(spoofing)   LOOP             2.2.2.9
Loop1                UP        UP(spoofing)   LOOP             --
Loop2                UP        UP(spoofing)   LOOP             --
M-E0/0/0             DOWN      DOWN           ETHERNET         --
NULL0                UP        UP(spoofing)   NULL             --
Tun3/0/20            DOWN      DOWN           TUNNEL           --
Vlan1                UP        UP             ETHERNET         192.168.0.73
Vlan2                DOWN      DOWN           ETHERNET         10.1.1.2
Vlan3                DOWN      DOWN           ETHERNET         20.1.1.1
Vlan100              DOWN      DOWN           ETHERNET         --
Vlan200              UP        DOWN           ETHERNET         --

The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
BAGG1                DOWN      auto         auto     access     1
Eth3/0/1             UP        100M(a)      full(a)  access     100
Eth3/0/2             UP        100M(a)      full(a)  access     200
Eth3/0/3             DOWN      auto         auto     hybrid     3
Eth3/0/4             DOWN      auto         auto     access     1
Eth3/0/5             DOWN      auto         auto     access     1
```

```
Eth3/0/6             DOWN      auto         auto     access     1
Eth3/0/7             DOWN      auto         auto     access     1
Eth3/0/8             DOWN      auto         auto     access     1
Eth3/0/9             DOWN      auto         auto     access     1
Eth3/0/10            DOWN      auto         auto     access     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             2.2.2.9
Loop1                UP        UP(spoofing)   LOOP             --
Loop2                UP        UP(spoofing)   LOOP             --
M-E0/0/0             DOWN      DOWN           ETHERNET         --
NULL0                UP        UP(spoofing)   NULL             --
Tun3/0/20            DOWN      DOWN           TUNNEL           --
Vlan1                UP        UP             ETHERNET         192.168.0.73
Vlan2                DOWN      DOWN           ETHERNET         10.1.1.2
Vlan3                DOWN      DOWN           ETHERNET         20.1.1.1
Vlan100              DOWN      DOWN           ETHERNET         --
Vlan200              UP        DOWN           ETHERNET         --
```

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             2.2.2.9
Loop1                UP        UP(spoofing)   LOOP             --
Loop2                UP        UP(spoofing)   LOOP             --
NULL0                UP        UP(spoofing)   NULL             --
Vlan1                UP        UP             ETHERNET         192.168.0.73
Vlan200              UP        DOWN           ETHERNET         --

The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
Eth3/0/1             UP        100M(a)      full(a)  access     100
Eth3/0/2             UP        100M(a)      full(a)  access     200
Eth3/0/48            UP        100M(a)      full(a)  access     1
```

Display the brief information of all interfaces excluding Ethernet interfaces.

```
<Sysname> display brief interface | exclude Eth
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
Loop0                UP        UP(spoofing)   LOOP             2.2.2.9
Loop1                UP        UP(spoofing)   LOOP             --
Loop2                UP        UP(spoofing)   LOOP             --
M-E0/0/0             DOWN      DOWN           ETHERNET         --
NULL0                UP        UP(spoofing)   NULL             --
Tun3/0/20            DOWN      DOWN           TUNNEL           --
```

```
Vlan1                UP         UP              ETHERNET         192.168.0.73
Vlan2                DOWN       DOWN            ETHERNET         10.1.1.2
Vlan3                DOWN       DOWN            ETHERNET         20.1.1.1
Vlan100              DOWN       DOWN            ETHERNET         --
Vlan200              UP         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
Main IP	Main IP
The brief information of interface(s) under bridge mode:	Brief information of interface(s) in bridge mode
Speed	Interface rate, in bps
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 Layer 2 interface Ethernet 2/0/1 and related information.

```
<Sysname> display interface ethernet 2/0/1
Ethernet2/0/1 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e200-8048
 Description: Ethernet2/0/1 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 9022
 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 10(sec)
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 100
 Port priority: 0
 Last 300 seconds input:  0 packets/sec 0 bytes/sec      -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec     -%
 Input (total):  0 packets, 0 bytes
          0 broadcasts, 0 multicasts
 Input (normal):  0 packets, - bytes
          0 broadcasts, 0 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 0 packets, 0 bytes
          0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, - bytes
          0 broadcasts, 0 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
Ethernet2/0/1 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)
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-down-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
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): 0 packets, 0 bytes 0 broadcasts, 0 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 broadcast packets, and multicast packets on the inbound direction of the interface
Input (normal): 0 packets, - bytes 0 broadcasts, 0 multicasts	Normal packet statistics on the inbound direction of the interface, including the statistics of normal packets and pause frames, in packets and bytes Number of 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

Field	Description
giants	Frames received that were longer than 1518 bytes (without VLAN tags) or 1522 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
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 1518 or 1522 bytes and contained checksum errors (the frame lengths in bytes may or may not be integers) • 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): 0 packets, 0 bytes 0 broadcasts, 0 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 broadcast packets, multicast packets, and pause frames on the outbound direction of the interface
Output (normal): 0 packets, - bytes 0 broadcasts, 0 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 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

Field	Description
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
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.

Field	Description
No port is detected with loopback	No port is currently being detected with a loopback.

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         GigabitEthernet0/0/25      GigabitEthernet0/0/18
       2         GigabitEthernet0/0/26      GigabitEthernet0/0/17
       3         GigabitEthernet0/0/27      GigabitEthernet0/0/20
       4         GigabitEthernet0/0/28      GigabitEthernet0/0/19
       5         GigabitEthernet0/0/29      GigabitEthernet0/0/22
       6         GigabitEthernet0/0/30      GigabitEthernet0/0/21
       7         GigabitEthernet0/0/31      GigabitEthernet0/0/24
       8         GigabitEthernet0/0/32      GigabitEthernet0/0/23
```

Table 1-4 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. The port number varies with device models. 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 interface ports included.
- If you provide the **all** keyword, this command displays the details for all manual port groups, including their names and the Ethernet interface 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):
    1                                    2
```

Display details of all the manual port groups.

```
<Sysname> display port-group manual all
 Member of 1:
    Ethernet2/0/1            Ethernet2/0/2            Ethernet2/0/3


 Member of 2:
    None
```

Display details of the port group named **group1**.

```
 Member of 1:
    Ethernet2/0/1            Ethernet2/0/2            Ethernet2/0/3
```

Table 1-5 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** | **unicast**] [**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.

unicast: Displays the information about storm constrain for unicast 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
Flow Statistic Interval: 10(second)
PortName      StormType LowerLimit UpperLimit Ctr-mode Status  Trap Log Swi-num
------------------------------------------------------------------------------
Eth2/0/5    broadcast 10         500        N/A     normal  on   on  0
```

Table 1-6 display storm-constrain command output description

Field	Description
Flow Statistic Interval	Interval for generating storm constrain statistics
PortName	Abbreviated port name
StormType	Type of the packets for which storm constrain function is enabled, which can be broadcast (for broadcast packets), multicast (for multicast packets), and unicast (for unicast packets).
LowerLimit	Lower threshold (in pps)
UpperLimit	Upper threshold (in pps)
Ctr-mode	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).

Field	Description
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.
Swi-num	Number of the forwarding state switching. This field is numbered modulo 65,535.

duplex

Syntax

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

undo duplex

View

Ethernet interface 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 interface of a Combo port does not support the **half** keyword.

Description

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

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

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

Related commands: **speed**.

Examples

Configure the interface Ethernet 2/0/1 to work in full-duplex mode.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] duplex full
```

flow-control

Syntax

flow-control

undo flow-control

View

Ethernet interface view

Default Level

2: System level

Parameters

None

Description

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

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

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

Note

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

Examples

Enable flow control on interface Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] flow-control
```

flow-interval

Syntax

flow-interval *interval*

undo flow-interval

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

interval: Time interval at which interface statistics are collected, in the range of 5 to 300 seconds, 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface 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 add an Ethernet interface to a specified manual port group.

Use the **undo group-member** command to remove a specified Ethernet interface from a manual port group.

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

Examples

Add interface Ethernet 2/0/1 to the manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member ethernet 2/0/1
```

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.

Examples

Enter Ethernet 2/0/1 interface view (assuming that the interface is a Layer 2 Ethernet interface).

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1]
```

jumboframe enable

Syntax

jumboframe enable [*value*]

undo jumboframe enable

View

Layer 2 Ethernet interface view, port group view

Default Level

2: System level

Parameters

value: Maximum length of Ethernet frames that are allowed to pass through. The effective range is 1,536 to 9,216 (in bytes).

Description

Use the **jumboframe enable** command to allow jumbo frames with the specified length to pass through an Ethernet interface.

Use the **undo jumboframe enable** command to prevent jumbo frames from passing through an Ethernet interface. That is, the maximum length of the frames allowed to pass through an Ethernet interface is 1518 bytes.

By default, the device allows frames no larger than 1536 bytes to pass through an Ethernet interface.

You can configure length of jumbo frames in global configuration mode (in system view) or on a port (in Ethernet interface view, port-group view) to allow them to pass through Ethernet interfaces.

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

Note

The latest configuration takes effect if you configure the *value* argument for multiple times in Ethernet interface view or port-group view.

Examples

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

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/0
[Sysname-port-group manual group1] jumboframe enable
```

Enable jumbo frames to pass through Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] jumboframe enable
```

link-delay

Syntax

link-delay *delay-time*

undo link-delay

View

Ethernet interface view

Default Level

2: System level

Parameters

delay-time: Up/down suppression time for the physical connection of the Ethernet interface (in seconds), in the range 0 to 30.

Description

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

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

By default, the suppression time is 0 second, that is, the physical layer will report physical-link-state changes without delay.

Examples

Set the up/down suppression time of the physical connection of interface Ethernet 2/0/1 to 8 seconds.

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

```
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] link-delay 8
```

loopback

Syntax

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

undo loopback

View

Ethernet interface view

Default Level

2: System level

Parameters

external: Enables external loopback testing on an Ethernet interface.

internal: Enables internal loopback testing on an Ethernet interface.

Description

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

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

By default, Ethernet interface loopback testing is disabled.

Note

- Ethernet interface loopback testing should be enabled while testing certain functionalities, such as during the initial identification of any network failure.
- While enabled, Ethernet interface 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] loopback internal
```

loopback-detection control enable

Syntax

loopback-detection control enable

undo loopback-detection control enable

View

Layer 2 Ethernet interface 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.

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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] loopback-detection enable
[Sysname-Ethernet2/0/1] loopback-detection control enable
```

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

System view, Layer 2 Ethernet interface 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.

With loopback detection enabled on a port (whose link type may be Access, Trunk, or Hybrid):

- If an Access port has been detected with loopback, it will transit to the loopback detection control state, where the incoming packets of the port are dropped and the outgoing packets of the port are forwarded normally. 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. If the loopback detection control function is enabled on the port, the port will transit to the loopback detection control state, where the incoming packets of the port are dropped and the outgoing packets of the port are forwarded normally. 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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

Layer 2 Ethernet interface 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 Ethernet 2/0/1 belongs.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] loopback-detection enable
[Sysname-Ethernet2/0/1] port link-type trunk
[Sysname-Ethernet2/0/1] loopback-detection per-vlan enable
```

mdi

Syntax

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

undo mdi

View

Layer 2 Ethernet interface 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 interface.

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

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

 **Note**

The command is not applicable to Combo ports operating as optical ports.

Examples

Set the MDI mode of Ethernet 2/0/1 to **across**.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] mdi across
```

multicast-suppression

Syntax

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

undo multicast-suppression

View

Layer 2 Ethernet interface view, port group view

Default Level

2: System level

Parameters

ratio: Maximum percentage of multicast traffic to the total transmission capability of an Ethernet interface, 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 the Ethernet interface(s) per second...

- For a 100-Mbps port, this value ranges from 1 to 148810 (in pps).
- For a 1-Gbps port, this value ranges from 1 to 1488100 (in pps).
- For a 10-Gbps port, this value ranges from 1 to 14881000 (in pps).

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 interface may not be the one that actually takes effect. To display the actual broadcast suppression threshold value on an Ethernet interface, 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 or keyword should be no smaller than 1, and the broadcast suppression threshold value is the one that actually takes effect on the Ethernet interface.

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 interface, that is, multicast traffic is not suppressed.

If you execute this command in Ethernet interface, 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 interface 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.
- On an Ethernet port enabled with multicast storm suppression ratio, this feature takes effect only in the inbound direction.

Examples

For Ethernet interface Ethernet 2/0/1, allow multicast traffic equivalent to 20% of the total transmission capability of Ethernet 2/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 ethernet 2/0/1
[Sysname-port-group-manual-group1] group-member ethernet 2/0/2
[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 Ethernet 2/0/1.

```
<Sysname> reset counters interface ethernet 2/0/1
```

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet interface view

Default Level

2: System level

Parameters

None

Description

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

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

By default, an Ethernet interface 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 double 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] shutdown
```

Bring up interface Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] undo shutdown
```

speed

Syntax

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

undo speed

View

Ethernet interface view

Default Level

2: System level

Parameters

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

100: Specifies the interface rate as 100 Mbps. The optical interface of a Combo 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 interface data rate.

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

By default, the port speed is in the auto-negotiation mode.

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

Note

You are recommended to configure the same port rate and duplex mode on two ports connected to each other, for example, set the duplex mode of both ports to auto negotiation or full/half duplex, so as to avoid packet loss.

Examples

Configure the interface rate as 100 Mbps for interface Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] speed 100
```

speed auto

Syntax

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

undo speed

View

100MB or Gigabit Layer 2 Ethernet interface 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 of the current interface.

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

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:

- When the auto-negotiation rate ranges set on the local and peer ends do not intersect, for example, 10 and 100 Mbps on one end and 1000 Mbps on the other, the rate negotiation will fail.
- When the auto-negotiation rate ranges set on the local and peer ends intersect, for example, 10 and 100 Mbps on one end and 100 and 1000 Mbps on the other, the negotiation rate range is the intersection, 100 Mbps.
- When the auto-negotiation rate ranges set on the local and peer ends are the same, for example, 100 and 1000 Mbps, the maximum value of the auto-negotiation rate is 1000 Mbps.

Note

- This function is available for auto-negotiation-capable 100 MB or Gigabit Layer-2 Ethernet interfaces only. For a Combo port, only the electrical port supports this function.
- If you repeatedly use the speed and the speed auto commands to configure the transmission rate on an interface, only the latest configuration takes effect.

Examples

Set the auto-negotiation rate of interface GigabitEthernet 2/0/1 to 10 Mbps or 1000 Mbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] speed auto 10 1000
```

storm-constrain

Syntax

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

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

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

all: Disables the storm constrain function for all types of packets (that is, unicast packets, 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 that the thresholds to be configured.

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

- For a 100-Mbps port, this value ranges from 1 to 148810.
- For a 1-Gbps port, this value ranges from 1 to 1488100.
- For a 10-Gbps port, this value ranges from 1 to 14881000.

min-pps-values: Lower threshold to be set, in pps. The range of this argument is 1 to *max-pps-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 **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 unicast packets on Ethernet 2/0/1, setting the upper and lower threshold to 200 pps and 150 pps.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] storm-constrain unicast pps 200 150
```

storm-constrain control

Syntax

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

undo storm-constrain control

View

Layer 2 Ethernet interface 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 Ethernet 2/0/1 when a type of traffic reaching it exceeds the corresponding upper threshold.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] storm-constrain control block
```

storm-constrain enable log

Syntax

storm-constrain enable log

undo storm-constrain enable log

View

Layer 2 Ethernet interface 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
```

```
[Sysname-Ethernet2/0/1] undo storm-constrain enable log
```

storm-constrain enable trap

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

View

Layer 2 Ethernet interface 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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

Layer 2 Ethernet interface view, port group view

Default Level

2: System level

Parameters

ratio: Maximum percentage of unicast traffic to the total transmission capability of an Ethernet interface, 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 interface per second.

- For a 100-Mbps port, this value ranges from 1 to 148810 (in pps).
- For a 1-Gbps port, this value ranges from 1 to 1488100 (in pps).
- For a 10-Gbps port, this value ranges from 1 to 14881000 (in pps).

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 interface may not be

the one that actually takes effect. To display the actual broadcast suppression threshold value on an Ethernet interface, 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 or keyword should be no smaller than 1, and the broadcast suppression threshold value is the one that actually takes effect on the Ethernet interface.

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 interface, that is, unicast traffic is not suppressed.

If you execute this command in Ethernet interface, 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 interface 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.
- On an Ethernet port enabled with unicast storm suppression ratio, this feature takes effect only in the inbound direction.

Examples

For Ethernet interface Ethernet 2/0/1, 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 ethernet 2/0/1
[Sysname-port-group-manual-group1] group-member ethernet 2/0/2
[Sysname-port-group-manual-group1] unicast-suppression 20
```

virtual-cable-test

Syntax

virtual-cable-test

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **virtual-cable-test** command to test the cable connected to the Ethernet interface 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

- The optical interface of a Combo port does not support this command. The support of other Ethernet interfaces for this command varies with device models.
- A link in the up state goes down and then up automatically if you execute this command on one of the Ethernet interfaces 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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

Table of Contents

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

Examples

Display the local system ID.

```
<Sysname> display lacp system-id
 Actor System ID: 0x8000, 000f-e200-0100
```

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

Field	Description
Actor System ID	The local system ID, which comprises the LACP system priority and the system 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 Ethernet 2/0/1, which is in a static aggregation group.

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

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

Ethernet2/0/1:
Aggregation Interface: Bridge-Aggregation1
Port Number: 1
Oper-Key: 1
```

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

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

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

Ethernet2/0/2:
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 1-2 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. • 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          NonS
BAGG10       D         0x8000, 000f-e267-57ad   2      0          Shar
```

Table 1-3 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
AGG Interface	Abbreviated name of the aggregate interface
AGG Mode	Aggregation group type

Field	Description
Partner ID	System ID of the partner
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. The value range is 1 to 1,024. 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* or **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** or **display link-aggregation verbose route-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
--------------------------------------------------------------------------------
  Eth2/0/6         U       32768    1         {ACG}
  Eth2/0/7         U       32768    1         {ACG}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  Eth2/0/6         0       32768    0         0x8000, 0000-0000-0000 {EF}
  Eth2/0/7         0       32768    0         0x8000, 0000-0000-0000 {EF}
```

Table 1-4 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.

Field	Description
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
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.
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 1,024..

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 Ethernet 1/0 to 64.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 port-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 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 1,024.

Description

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

Use the **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 Ethernet 2/0/1 to aggregation group 22.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-aggregation group 22
```

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.

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

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
```

Table of Contents

1 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
    Ethernet2/0/4            Ethernet2/0/5
```

Table 1-1 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
Ethernet2/0/4 Ethernet2/0/5	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

group *group-number*: Specifies the ID of the group to which the ports are to be added. The value range varies with devices.

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*.

Note that: This command adds a port to the default isolation group (isolation group 1).

Examples

Assign ports Ethernet 2/0/1 to the isolation group.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port-isolate enable
```

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 ethernet 2/0/2
[Sysname-port-group-manual-aa] group-member ethernet 2/0/3
[Sysname-port-group-manual-aa] group-member ethernet 2/0/4
[Sysname-port-group-manual-aa] port-isolate enable
```

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

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] quit
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] port link-aggregation group 1
[Sysname-Ethernet2/0/1] quit
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] port link-aggregation group 1
[Sysname-Ethernet2/0/2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port-isolate enable
```

Table of Contents

1 Service Loopback Group Configuration Commands

Service Loopback Group Configuration Commands

display service-loopback group

Syntax

display service-loopback group [*number*]

View

Any view

Default Level

1: Monitor level

Parameters

number: ID of the service loopback group to be displayed. The range of the *number* argument is 1 to 1,024.

Description

Use the **display service-loopback group** command to display information of the specified service loopback group. If no service loopback group is specified, information of all service loopback groups is displayed.

Examples

Display information of service loopback group 5.

```
<Sysname> display service-loopback group 5
Service Group ID:    5        Quote Number: 0
Service Type: tunnel
  Member                                                    Status
------------------------------------------------------------------------------
  Eth2/0/1                                                  Selected
  Eth2/0/2                                                  Selected
```

Table 1-1 display service-loopback group command output description

Field	Description
Service Group ID	Service loopback group ID
Quote Number	Reference count of the service loopback group
Service Type	Service type of the service loopback group

Field	Description
Member	Member ports of the service loopback group
Status	Port state, which can be selected or unselected

port service-loopback group

Syntax

port service-loopback group *number*

undo port service-loopback group

View

Ethernet interface view

Default Level

2: System level

Parameters

number: Service loopback group ID. The value range for the *number* argument is 1 to 1,024..

Description

Use the **port service-loopback group** command to assign the Layer-2 Ethernet interface to the specified service loopback group.

Use the **undo port service-loopback group** command to remove the Layer-2 Ethernet interface from the specified service loopback group.

Note that you cannot remove the last member port of a referenced service loopback group.

Examples

Assign Layer-2 Ethernet interface Ethernet 2/0/1 to service loopback group 1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] port service-loopback group 1
```

service-loopback group

Syntax

service-loopback group *number* **type** { **multicast-tunnel** | **tunnel** } *

undo service-loopback group *number*

View

System view

Default Level

2: System level

Parameters

number: Service loopback group ID. The value range for the *number* argument is 1 to 1,024..

type: Specifies the service type of a service loopback group.

tunnel: Specifies the service type of a service loopback group as Tunnel.

multicast-tunnel: Specifies the service type of a service loopback group as Multicast tunnel.

Description

Use the **service-loopback group** command to create a service loopback group or change the service type of an existing service loopback group.

Use the **undo service-loopback group** command to remove a service loopback group.

Note that:

- A service loopback group can be referenced by other features after its creation. Only after being referenced can a service loopback group process service traffic. A service loopback group can be referenced by multiple features at the same time.
- You can change the service type of an existing service loopback group. For the change to be successful, you must ensure that the service group has not been referenced; the attributes of all member ports (if any) are not conflicting with the target service type; and no service loopback group has been created for the target service type, because only one service loopback group is allowed for a service type.
- You can remove any service loopback group except the referenced ones.

Examples

Configure service loopback group 1 to support the tunnel service.

```
<Sysname> system-view
[Sysname] service-loopback group 1 type tunnel
```

Table of Contents

1 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 GigabitEthernet2/0/1
 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 GigabitEthernet2/0/2
 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 GigabitEthernet2/0/1.

```
<Sysname> display dldp GigabitEthernet 2/0/1
Interface GigabitEthernet2/0/1
 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 1-1 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 GigabitEthernet2/0/1
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 3

Interface GigabitEthernet2/0/2
 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 2/0/1.

```
<Sysname> display dldp statistics GigabitEthernet 2/0/1
Interface GigabitEthernet2/0/1
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 3
```

Table 1-2 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 these two commands apply to all the 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.

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.

By default, DLDP is disabled globally or on a port.

Note

- 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.

```
<Sysname> system-view
[Sysname] dldp enable
```

Enable DLDP on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] dldp enable
```

Enable DLDP for all the ports in port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member GigabitEthernet 2/0/1 to GigabitEthernet 2/0/3
[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 the 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.

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 2/0/1 (assuming that GigabitEthernet 2/0/1 is shut down by DLDP).

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 to GigabitEthernet 2/0/3
[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. When a device operates in this mode and a neighbor entry it maintains expires, the device detects the neighbor before removing the neighbor entry.

normal: Specifies the normal DLDP mode. When a device operates in this mode and a neighbor entry it maintains expires, the device removes the neighbor entry directly.

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.

Note that:

- In normal DLDP mode, only fiber cross-connected unidirectional links can be detected.
- In enhanced DLDP mode, two types of unidirectional links can be detected. One is fiber cross-connected links. The other refers to fiber pairs with one fiber not connected or disconnected.

Note

The support for these two commands varies with device models.

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
```

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    : GigabitEthernet2/0/1
 Receiving time of the last flush packet         : 19:19:03 2008/06/27
 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 48.

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
 ------------------------------------------------------------------------------
 GigabitEthernet2/0/1      MASTER  ACTVIE    1        16:37:20 2008/04/21
 GigabitEthernet2/0/2     SLAVE  STANDBY     2        17:45:20 2008/04/21
```

Table 1-2 display smart-link group command output description

Field	Description
Smart link group 1 information	Information about smart link group 1
Device ID	Device ID
Preemption mode	Preemption mode, which can be **role** for preemption enabled or none for preemption disabled.
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 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	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. If no VLAN is specified, VLAN 1 applies by default.

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.

Different smart link groups must be configured with different control VLANs.

Related commands: **smart-link flush enable**.

Examples

Enable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] 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 2/0/1 as the slave port of smart link group 1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp disable
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port GigabitEthernet 2/0/1 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 48.

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 2/0/1 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 2/0/1
[Sysname-GigabitEthernet2/0/1] stp disable
[Sysname-GigabitEthernet2/0/1] 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] stp disable
[Sysname-Bridge-Aggregation1] port smart-link group 1 master
```

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 the role preemption mode.

Use the **undo preemption mode** command to restore the default.

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 2/0/1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 48.

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.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1]
```

Table of Contents

1 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.

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use the **display lldp local-information** command to display the global LLDP information or the information contained in the LLDP TLVs to be sent to neighboring devices through a port.

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.

Examples

Display all the LLDP information to be sent.

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID         : 000f-e218-d0d1
  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               : VER.A
  FirmwareRev               : 202
  SoftwareRev               : S7900E
```

```
  SerialNum                 : Unknown
  Manufacturer name         : Unknown
  Model name                : Unknown
  Asset tracking identifier : Unknown
LLDP local-information of port 97[GigabitEthernet2/0/1]:
  Port ID subtype  : Interface name
  Port ID          : GigabitEthernet2/0/1
  Port description : GigabitEthernet2/0/1 Interface

  Management address type           : ipV4
  Management address                : 192.168.0.72
  Management address interface type : IfIndex
  Management address interface ID   : 51
  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(100)/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 1-1 display lldp local-information command output description

Field	Description
Global LLDP local-information	The global LLDP information
Chassis ID	ID that identifies the LLDP sending device
System name	System name of the device
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.
PoE device type	PoE device type
MED information	MED information
Device class	MED 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 stream. • 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 board
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 number *interface-type interface-number*	LLDP information about a port
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
Port description	Port description

Field	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 ID	Name of the VLAN identified by the VLAN ID
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
Power port class	PoE device type, which can be : • PSE, indicating a power supply device • PD, indicating a 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** or **Spare**.
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 voice VLAN are tagged.
Media Policy VlanID	ID of the voice VLAN
Media Policy L2 priority	Layer 2 priority
Media Policy Dscp	DSCP precedence
Location format	Location 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 telephone number for urgencies.
Location Information	Location information
PoE PSE power source	PSE type, which can be: • Primary, indicating a primary power supply • Backup, indicating a backup power supply
Port PSE Priority	Port PSE priority, which can be : • Unknown • Critical • High • Low
Port Available power value	PoE power

display lldp neighbor-information

Syntax

display lldp neighbor-information [**interface** *interface-type interface-number*] [**brief**]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

brief: Displays the LLDP information in brief.

Description

Use the **display lldp neighbor-information** command to display the LLDP information about the neighboring devices received through a port.

With no keyword/argument specified, this command displays the LLDP information received through all the ports.

Examples

Display the LLDP information received through all the ports.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 144[GigabitEthernet2/0/48]:
  Neighbor index   : 1
  Update time      : 0 days,1 hours,45 minutes,4 seconds
  Chassis type     : MAC address
  Chassis ID       : 000f-e22e-972b
  Port ID type     : Interface name
  Port ID          : GigabitEthernet3/0/48
  Port description : GigabitEthernet3/0/48 Interface
  System name        : System
  System description : System
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  Management address type           : ipV4
  Management address                : 192.168.0.74
  Management address interface type : IfIndex
  Management address interface ID   : 347
  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
```

Table 1-2 display lldp neighbor-information command output description

Field	Description
LLDP neighbor-information	LLDP information about a neighboring device
LLDP neighbor-information of Port number *interface-type interface number*	LLDP information received through a specific port
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.
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: • Bridge, indicating switching • Router, indicating routing

Field	Description
System capabilities enabled	Capabilities currently enabled on the neighboring device, which can be: • 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 he port VLAN
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, indicating a power supply device. • PD, indicating a 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** or **Spare**.
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

Field	Description
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 stream. • 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.
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 device can acquire media policy data
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
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNumber	Serial number
Manufacturer name	Manufacturer name
Model name	Module name
Asset tracking identifier	Asset tracking ID
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.

Field	Description
Location Information	Location information
PoE PSE power source	PSE 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	Port PSE priority, which can be: • Unknown • Critical • High • Low
Available power value	PoE power
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 organization-defined TLV
TLV OUI	OUI of the unknown organization-defined TLV
TLV subtype	Unknown organization-defined TLV subtype
Index	Unknown organization index
TLV information	Information contained in unknown organization-defined TLV

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,1 hours,45 minutes,5 seconds
The number of LLDP neighbor information inserted : 6
The number of LLDP neighbor information deleted  : 3
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 0

LLDP statistics Information of port 97 [GigabitEthernet2/0/1]:
The number of LLDP frames transmitted            : 175
The number of LLDP frames received               : 517
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
```

(The subsequent output, if any, is omitted.)

Table 1-3 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 number *interface-type interface-number*	LLDP statistics of a port
The number of LLDP frames transmitted	Total number of the LLDP frames transmitted through the port
The number of LLDP frames received	Total number of the LLDP frames received through the port
The number of LLDP frames discarded	Total number of the LLDP frames dropped on the port

Field	Description
The number of LLDP error frames	Total number of the LLDP error frames received through the port
The number of LLDP TLVs discarded	Total number of the LLDP TLVs dropped on the port
The number of LLDP TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized on the port
The number of LLDP neighbor information aged out	Number of the LLDP neighbor information entries that have aged out on the port
The number of CDP frames transmitted	Total number of the CDP frames transmitted on the port
The number of CDP frames received	Total number of the CDP frames received on the port
The number of CDP frames discarded	Total number of the CDP frames dropped on the port
The number of CDP error frames	Total number of the CDP error frames received on the port

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: 3
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days,1 hours,45 minutes,5 seconds
Transmit interval              : 30s
Hold multiplier                : 4
Reinit delay                   : 2s
```

```
Transmit delay                : 2s
Trap interval                 : 5s
Fast start times              : 3

Port 97 [GigabitEthernet2/0/1]:
Port status of LLDP           : Enable
Admin status                  : Tx_Rx
Trap flag                     : No
Roll time                     : 0s

Number of neighbors:            1
Number of MED neighbors       : 0
Number of CDP neighbors       : 0
Number of sent optional TLV   : 22
Number of received unknown TLV : 0
```

Table 1-4 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	The last changed time of LLDP neighbor information
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
Port number *interface-type interface-number*	Port LLDP status
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.
Roll time	LLDP polling interval. A value of 0 indicates LLDP polling is disabled.

Field	Description
Number of neighbors	Number of the LLDP neighbors connecting to the port
Number of MED neighbors	Number of the 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 TLVs that are currently sent through a port.

If no port is specified, this command displays all the TLVs that are currently sent through all the ports.

Examples

Display all the TLVs that are currently sent through all the ports.

```
<Sysname> display lldp tlv-config
LLDP tlv-config of port 97[GigabitEthernet2/0/1]:
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
```

(The subsequent output, if any, is omitted.)

Table 1-5 display lldp tlv-config command output description

Field	Description
LLDP tlv-config of port number *interface-type interface-number*	TLVs that are currently sent through a port
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 extended TLVs, including: • Port VLAN ID TLV • Port and protocol VLAN ID TLV • VLAN name TLV
IEEE 802.3 extended TLV	IEEE 802.3 extended 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 • Location Identification TLV • Extended Power-via-MDI 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 GigabitEthernet 2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] lldp admin-status rx
```

lldp check-change-interval

Syntax

lldp check-change-interval *value*

undo lldp check-change-interval

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

value: 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 GigabitEthernet2/0/3, setting the polling interval to 30 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] 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).

Examples

Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 global CDP compatibility.

Use the **undo lldp compliance cdp** command to restore the default.

By default, global CDP compatibility is disabled.

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 enabled at both the global and port levels.

Note that LLDP takes effect on a port only when it is enabled both globally and on the port.

Examples

Disable LLDP on GigabitEthernet 2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] 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 GigabitEthernet 2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] lldp encapsulation snap
```

lldp fast-count

Syntax

lldp fast-count *value*

undo lldp fast-count

View

System view

Default level

2: System level

Parameters

value: 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 GigabitEthernet 2/0/3 to encapsulate the management address in the form of strings in management address TLVs.

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

```
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] 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 least 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. For information about VLAN, refer to *VLAN Configuration* in the *Access Volume*.

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 GigabitEthernet2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] 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 trap for GigabitEthernet2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] lldp notification remote-change enable
```

lldp timer notification-interval

Syntax

lldp timer notification-interval *value*

undo lldp timer notification-interval

View

System view

Default level

2: System level

Parameters

value: Interval to send trap messages, in the range 5 to 3600 (in seconds).

Description

Use the **lldp timer notification-interval** command to set the interval to send trap messages.

Use the **undo lldp timer notification-interval** command to restore the default.

By default, the interval to send trap messages is 5 seconds.

Examples

Set the interval to send trap messages to 8 seconds.

```
<Sysname> system-view
[Sysname] lldp timer notification-interval 8
```

lldp timer reinit-delay

Syntax

lldp timer reinit-delay *value*

undo lldp timer reinit-delay

View

System view

Default level

2: System level

Parameters

value: 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 *value*

undo lldp timer tx-delay

View

System view

Default level

2: System level

Parameters

value: 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 *value*

undo lldp timer tx-interval

View

System view

Default level

2: System level

Parameters

value: 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 defined LLDP TLVs, or all the IEEE 802.3 defined LLDP TLVs; or sends all the MED related LLDP TLVs except location identification TLVs.

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 defined 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 the TLVs (port and protocol VLAN ID TLVs or VLAN name TLVs) concerning which are to be sent. This argument defaults to the least protocol VLAN ID.

dot3-tlv: Sends IEEE 802.3 defined 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 enable the sending of specific 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 sent.

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.
- Specifying the **all** keyword for basic LLDP TLVs and organization defined LLDP TLVs (including IEEE 802.1 defined LLDP TLVs and IEEE 802.3 defined LLDP TLVs) enables sending of all the corresponding LLDP TLVs. For MED related LLDP TLVs, the **all** keyword enables sending of all the MED related LLDP TLVs except location identification TLVs.
- 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 on GigabitEthernet 2/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet2/0/3
[Sysname-GigabitEthernet2/0/3] lldp tlv-enable dot3-tlv link-aggregation
```

Table of Contents

1 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: Description of a VLAN or VLAN interface. 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.

- For a VLAN, the description string contains 1 to 32 characters.
- For a VLAN interface, the description string contains 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.

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: UP
Line protocol current state: UP
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet Address is 192.168.0.72/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0000-fc00-6505
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0000-fc00-6505
```

Table 1-1 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.

Field	Description
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.
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.

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 reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. You cannot do any operation 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
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet2/0/1      GigabitEthernet2/0/3       GigabitEthernet2/0/4
```

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
 Tagged   Ports: none
 Untagged Ports: none
```

Table 1-2 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
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.

When a VLAN connects to one subnet, you need to assign only one IP address for its VLAN interface. When the VLAN connects to multiple subnets, you need to assign multiple IP addresses for the VLAN interface. On an S7900E series Ethernet switch, you can assign up to five IP addresses to a VLAN interface.Among these IP addresses, one is primary and the others are secondary.

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
```

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.

all: Creates or removes all VLANs except reserved VLANs.

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.
- If an isolate-user-VLAN and a secondary VLAN are associated with each other with the **isolate-user-vlan** command, the isolate-user-VLAN or secondary VLAN cannot be removed unless the association is removed first.

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
GE2/0/2              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                              2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                              150-160, 200, 255, 286, 300-302
```

Display information about the trunk ports in the system.

```
<Sysname> display port trunk
Interface            PVID  VLAN passing
GE2/0/1              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 1-3 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**.
- If you use this command to assign a Layer-2 aggregate interface to a VLAN, this command assigns the Layer-2 aggregate interface but not its member ports to the current VLAN. For detailed information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **display vlan**.

Examples

Assign GigabitEthernet 2/0/1 through GigabitEthernet 2/0/3 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
```

```
[Sysname-vlan2] port GigabitEthernet 2/0/1 to GigabitEthernet 2/0/3
```

Assign Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port bridge-aggregation 1
```

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 Ethernet interface view, this command only applies to the current 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*.

Examples

Assign GigabitEthernet 2/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 Ethernet interface view, this command only applies to the current 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 2/0/1.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type hybrid
[Sysname-GigabitEthernet2/0/1] 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 Ethernet interface view, this command only applies to the current 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*.

Related commands: **port link-type**.

Examples

Assign the hybrid port GigabitEthernet 2/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100, and configure GigabitEthernet 2/0/1 to send packets of these VLANs with tags kept.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type hybrid
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 to GigabitEthernet 2/0/6
[Sysname-port-group-manual-2] port link-type hybrid
[Sysname-port-group-manual-2] port hybrid vlan 2 untagged
 Configuring GigabitEthernet2/0/1... Done.
 Configuring GigabitEthernet2/0/2... Done.
 Configuring GigabitEthernet2/0/3... Done.
 Configuring GigabitEthernet2/0/4... Done.
 Configuring GigabitEthernet2/0/5... Done.
 Configuring GigabitEthernet2/0/6... 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 GigabitEthernet2/0/1... Done.
 Configuring GigabitEthernet2/0/2... Done.
```

Note that GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2 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 Ethernet interface view, this command only applies to the current 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 2/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 ethernet 2/0/1
[Sysname-port-group manual group1] group-member ethernet 2/0/2
[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 Ethernet interface view, this command only applies to the current 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*.

Related commands: **port link-type**.

Examples

Assign the trunk port GigabitEthernet 2/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 is an access port, and GigabitEthernet 2/0/2 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 GigabitEthernet2/0/1! This port is not a Trunk port!
 Configuring GigabitEthernet2/0/1... 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 GigabitEthernet2/0/1! This port is not a Trunk port!” indicates that the configuration failed on GigabitEthernet 2/0/1 because GigabitEthernet 2/0/1 was not a trunk port; “Configuring Ethernet GigabitEthernet 2/0/2... Done” indicates that the configuration on GigabitEthernet 2/0/2 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 Ethernet interface view, this command only applies to the current 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 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 is an access port and GigabitEthernet 2/0/2 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 GigabitEthernet2/0/1! This port is not a Trunk port!
```

The output above shows that the configuration on Bridge-aggregation 1 and the member port GigabitEthernet 2/0/2 succeeded; the configuration on GigabitEthernet 2/0/1 failed because GigabitEthernet 2/0/1 was not a trunk port.

MAC Address-Based VLAN Configuration Commands

display mac-vlan

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **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.

mask *mac-mask*: Displays the MAC address-to-VLAN entries with their MAC addresses in the specified range.

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
------------------------------------------------------------------------
0008-0001-0000     FFFF-FF00-0000         5         3       S
0002-0001-0000     FFFF-FFFF-FFFF         5         3       S&D

Total MAC VLAN address count:2
```

Table 1-4 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:
----------------------------------------
 GigabitEthernet2/0/1  GigabitEthernet2/0/2  GigabitEthernet2/0/3
```

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 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname–GigabitEthernet2/0/1] mac-vlan enable
```

mac-vlan mac-address

Syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri*]

undo mac-vlan { **all** | **mac-address** *mac-address* [**mask** *mac-mask*] | **vlan** *vlan-id* }

View

System view

Default Level

2: System level

Parameters

mac-address *mac-address*: Specifies a MAC address.

mask *mac-mask*: Specifies a mask for the MAC address in the format of H-H-H. The *mac-mask* argument is comprised of the high-order part (all the binary bits of which are **1**s) and the low-order part (all the binary bits of which are **0**s). By default, the hexadecimal digits of this argument are all **F**s.

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.

Two MAC address-to-VLAN entry tables exist in a device. One table contains the MAC address-to-VLAN entries configured with the **mask** keyword specified. A MAC address-to-VLAN entry of this type describes the relationship between a group of MAC addresses and a VLAN, and a priority value. Another table contains the MAC address-to-VLAN entries configured without the **mask** keyword specified. A MAC address-to-VLAN entry of this type describes the relationship between a single MAC address and a VLAN, and a priority value. The system adds/removes MAC address-to-VLAN entries to/from the two tables according to your configuration.

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
```

Associate the MAC addresses with the high-order six hexadecimal digits being 111122 with VLAN 100 and 802.1p priority 4.

```
<Sysname> system-view
[Sysname] mac-vlan mac-address 1111-2222-3333 mask ffff-ff00-0000 vlan 100 priority 4
```

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 MAC address-based VLANs and IP subnet-based VLANs are created on a port, MAC address-to-VLAN entries configured with the **mask** keyword specified are matched preferentially, and the left VLAN entries are matched as configured by the **vlan precedence** command.

Examples

Configure to match VLANs based on MAC addresses preferentially on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1.

```
[Sysname] display protocol-vlan interface GigabitEthernet 2/0/1
 Interface: GigabitEthernet2/0/1
   VLAN ID   Protocol Index      Protocol Type
 ============================================================
       3          0               ipv4
```

The sample output shows that untagged packets received on GigabitEthernet 2/0/1 will be tagged with VLAN ID 2 if they carry AppleTalk packets or with VLAN ID 3 if they carry IPv4 packets.

Table 1-5 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
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
          3              ipx ethernetii
 VLAN ID:3
    Protocol Index      Protocol Type
 ======================================================
          0              ipv4
          1              ipx snap
```

Refer to Table 1-5 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, in the range 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. The *protocol-end* argument must be greater than or equal to the beginning protocol index. The range of the *protocol-end* argument varies with device models.

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 Ethernet interface view, this command only applies to the current 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*.

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.

Note

At present, the AppleTalk-based protocol template cannot be associated with a port on an S7900E series Ethernet switch.

Related commands: **display protocol-vlan interface**.

Examples

Associate the hybrid port GigabitEthernet 2/0/1 with protocol 0 in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan ipv4
[Sysname-Vlan2] quit
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type hybrid
[Sysname-GigabitEthernet2/0/1] port hybrid vlan 2 untagged
 Please wait... Done
[Sysname-GigabitEthernet2/0/1] 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**, Ethernet 6/0/2 is an access port and Ethernet 6/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan ipv4
[Sysname-Vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation2] port link-type access
 Please wait... Done.
 Configuring GigabitEthernet2/0/1... Done.
 Configuring GigabitEthernet2/0/1.............................. Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done.
 Configuring GigabitEthernet2/0/1... Done.
```

```
 Configuring GigabitEthernet2/0/1... 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, which specifies the protocol template to be bound with the current VLAN, in the range 0 to 15. System will automatically assign an index if this parameter is not specified.

to *protocol-end*: Specifies the end protocol index, in the range 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-type interface-number1* [**to** *interface-type interface-number2* | **all** }

View

Any view

Default Level

2: System level

Parameters

interface-type interface-number1: Specifies a port by its type and number.

interface-type interface-number1 **to** *Interface-type interface-number2*: Specifies multiple ports.

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 2/0/1.

```
<Sysname> system-view
[Sysname]display ip-subnet-vlan interface gigabitethernet2/0/1
Interface: GigabitEthernet2/0/1
  VLAN ID   Subnet-Index    IP ADDRESS        NET MASK
  ========================================================
     3           0            192.168.1.0    255.255.255.0
```

Table 1-6 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 1-7 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 Ethernet interface view, this command only applies to the current 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*.

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 2/0/1 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 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type hybrid
[Sysname-GigabitEthernet2/0/1] port hybrid vlan 3 untagged
 Please wait... Done.
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 is an access port and GigabitEthernet 2/0/2 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 GigabitEthernet 2/0/1... Done.
 Configuring GigabitEthernet 2/0/2.......................... Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
Please wait... Done.
 Configuring GigabitEthernet 2/0/1... Done.
 Configuring GigabitEthernet 2/0/2... Done.
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

2 Super VLAN Configuration Commands

Super VLAN Configuration Commands

display supervlan

Syntax

display supervlan [*supervlan-id*]

View

Any view

Default Level

1: Monitor level

Parameters

supervlan-id: Super VLAN ID, in the range of 1 to 4094.

Description

Use the **display supervlan** command to display the mapping between a super VLAN and sub-VLANs, and the information of these VLANs.

Related commands: **supervlan**, **subvlan**.

Examples

Display the mapping between a super VLAN and sub-VLANs.

```
<Sysname> display supervlan 2
 Supervlan ID :  2
Subvlan ID :  3-5

 VLAN ID: 2
 VLAN Type: static
 It is a Super VLAN.
Route Interface: configured
 IP Address: 10.153.17.41
 Subnet Mask: 255.255.252.0
 Description: VLAN 0002
 Tagged   Ports: none
 Untagged Ports: none

 VLAN ID: 3
 VLAN Type: static
 It is a Sub VLAN.
 Route Interface: not configured
```

```
Description: VLAN 0003
Tagged   Ports: none
Untagged Ports:
            GigabitEthernet2/0/3

VLAN ID: 4
VLAN Type: static
It is a Sub VLAN.
Route Interface: not configured
Description: VLAN 0004
Tagged   Ports: none
Untagged Ports:
            GigabitEthernet2/0/4

VLAN ID: 5
VLAN Type: static
It is a Sub VLAN.
Route Interface: not configured
Description: VLAN 0005
Tagged   Ports: none
Untagged Ports:
            GigabitEthernet2/0/5
```

Table 2-1 display supervlan command output description

Field	Description
Supervlan ID	Super VLAN ID
Subvlan ID	Sub-VLAN ID
VLAN ID	VLAN ID
VLAN Type	VLAN type, static or dynamic
Route Interface	Whether a VLAN interface is configured for the current VLAN. This field is the same for both sub-VLANs and the super VLAN.
IP Address	IP address of the VLAN interface, if configured. This field is the same for both sub-VLANs and the super VLAN.
Subnet Mask	Subnet mask of the VLAN interface, if configured. This field is the same for both sub-VLANs and the super VLAN.
Description	VLAN description
Tagged Ports	Ports through which packets of the VLAN are sent tagged.
Untagged Ports	Ports through which packets of this VLAN are sent untagged

subvlan

Syntax

subvlan *vlan-list*

undo subvlan [*vlan-list*]

View

VLAN view

Default Level

2: System level

Parameters

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

Description

Use the **subvlan** command to associate the super VLAN with the specified sub-VLAN (s).

The current VLAN is the super VLAN whereas the VLANs specified by the *vlan-list* paramter are the sub-VLANs.

Use the **undo subvlan** command to remove the association.

Note:

- Ensure that the sub-VLANs already exist before associating them with a super VLAN.
- You can add/remove a port to/from a sub-VLAN already associated with a super VLAN.
- The **undo subvlan** command without *vlan-list* specified removes the association between the specified super VLAN and all its sub-VLANs, while the **undo subvlan** command with *vlan-list* specified only removes the association between the current super VLAN and the sub-VLANs specified by *vlan-list*.

Related commands: **display supervlan**.

Examples

Associate VLAN 10 (the super VLAN) with VLAN 3, VLAN 4, VLAN 5, and VLAN 9 (the sub-VLANs).

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] subvlan 3 to 5 9
```

supervlan

Syntax

supervlan

undo supervlan

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **supervlan** command to configure the current VLAN as a super VLAN.

Use the **undo supervlan** command to remove the super VLAN configuration for the current VLAN.

Note that:

- You cannot configure a super VLAN as the guest VLAN for a port, and vice versa. For more information about guest VLAN, refer to *802.1X Configuration* in the *Security Volume*.
- You can configure Layer 2 multicast for a super VLAN. However, the configuration cannot take effect.
- You can configure DHCP, Layer 3 multicast, dynamic routing, and NAT for the VLAN interface of a super VLAN. However, only DHCP can take effect.
- Configuring VRRP for the VLAN interface of a super VLAN affects network performance. Therefore, it is not recommended to configure this function.

Related commands: **display supervlan**.

Examples

Configure VLAN 2 as a super VLAN.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] supervlan
```

3 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
 Broadcast MAX-ratio: 100%
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet2/0/2       GigabitEthernet2/0/3      GigabitEthernet2/0/4

 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
 Broadcast MAX-ratio: 100%
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet2/0/2            GigabitEthernet2/0/3

 VLAN ID: 4
 VLAN Type: static
 Isolate-user-VLAN type : secondary
 Route Interface: not configured
 Description: VLAN 0004
 Broadcast MAX-ratio: 100%
 Tagged   Ports: none
 Untagged Ports:
GigabitEthernet2/0/2            GigabitEthernet2/0/4
```

Table 3-1 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
Subnet Mask	Subnet mask of the VLAN interface, if configured
Description	VLAN description
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-list*

undo isolate-user-vlan *isolate-user-vlan-id* [**secondary** *secondary-vlan-id-list*]

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-list*: Specifies a list of secondary VLAN IDs. You need to provide the *secondary-vlan-id* argument in the form of { *secondary-vlan-id1* [**to** *secondary-vlan-id2*] }&<1-10>, where *secondary-vlan-id1* and *secondary-vlan-id2* are VLAN IDs in the range 1 to 4094 and &<1-10> means that you can provide up to ten secondary VLAN IDs/secondary VLAN ID ranges.

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. 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 2/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port GigabitEthernet 2/0/3
[Sysname-vlan3] vlan 4
[Sysname-vlan4] port GigabitEthernet 2/0/4
```

```
[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 **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
```

4 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**, **voice vlan enable**.

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 4-1 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
Voice VLAN status: ENABLE
Voice VLAN ID: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT                     MODE
--------------------------------
GigabitEthernet2/0/2     MANUAL
GigabitEthernet2/0/3     MANUAL
GigabitEthernet2/0/4     MANUAL
GigabitEthernet2/0/5     AUTO
```

Table 4-2 display voice vlan state command output description

Field	Description
Voice VLAN status	The current voice VLAN status: ENABLE or DISABLE.
Voice VLAN ID	ID of the voice VLAN
Voice VLAN security mode	Security mode for the voice VLAN
Voice VLAN aging time	Aging time of the voice VLAN
Current voice vlan enabled port and its mode	Voice VLAN-enabled port and its voice VLAN mode
PORT	Port name
MODE	Voice VLAN mode of the port: manual or automatic.

voice vlan

Syntax

voice vlan *vlan-id* **enable**

undo voice vlan enable

View

System view

Default Level

2: System level

Parameters

vlan-id: ID of the VLAN to be enabled with the voice VLAN feature, in the range of 2 to 4094.

Description

Use the **voice vlan** command to enable the voice VLAN feature globally.

Use the **undo voice vlan enable** command to disable the voice VLAN feature globally.

- At a moment, only one VLAN can be enabled with the voice VLAN feature on a device.
- The VLAN to be configured as the voice VLAN must already exist and cannot be VLAN 1.
- To remove a voice VLAN, .disable the voice VLAN feature on the VLAN first.

Related commands: **display voice vlan state**.

Examples

Enable the voice VLAN feature on VLAN 2 (assuming that VLAN 2 already exists).

```
<Sysname> system-view
[Sysname] voice vlan 2 enable
```

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 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.

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 enable

undo voice vlan enable

View

Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **voice vlan enable** command to enable the voice VLAN feature on an Ethernet port.

Use the **undo voice vlan enable** command to disable the voice VLAN feature on an Ethernet port.

The voice VLAN feature is not enabled on a port by default.

- You cannot enable the voice VLAN feature on an access port operating in automatic voice VLAN mode.
- Enable the voice VLAN feature globally before enabling the voice VLAN feature on a port.
- The voice VLAN functions properly only after the voice VLAN feature is enabled both globally and on a port.

Examples

Enable the voice VLAN feature on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] voice vlan 2 enable
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] voice vlan enable
```

voice vlan mac-address

Syntax

voice vlan mac-address *mac-addr* **mask** *oui-mask* [**description** *text*]

undo voice vlan mac-address *oui*

View

System view

Default Level

2: System level

Parameters

mac-addr: 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, with the high-order bits being consecutive **f**s and the low-order bits being **0**s, for example, ffff-f000-0000.

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-addr* 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 4-3. You can remove the default OUI addresses and then add recognizable OUI addresses manually.

Table 4-3 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	0060-b900-0000	Philips/NEC phone
5	00d0-1e00-0000	Pingtel 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
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
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 mode.

Use the **undo voice vlan mode auto** command to configure the current port to operate in manual voice VLAN mode.

By default, a port operates in automatic voice VLAN 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 mode, you need to assign the port to the voice VLAN manually.

Examples

Configure GigabitEthernet 2/0/1 to operate in manual voice VLAN mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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.

Note

Only the **voice vlan security enable** command or the **undo voice vlan security enable** command issued before the **voice vlan** *vlan-id* **enable** command takes effect.

Examples

Disable voice VLAN security mode.

```
<Sysname> system-view
[Sysname] undo voice vlan security enable
```

Table of Contents

1 GARP/GVRP Configuration Commands

GARP 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.

Examples

Display statistics about GARP for port GigabitEthernet 2/0/1.

```
<Sysname> display garp statistics interface GigabitEthernet2/0/1
        GARP statistics on port GigabitEthernet2/0/1
```

```
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.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP timer settings of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command displays the GARP timer settings of the specified ports.

Related commands: **garp timer**, **garp timer leaveall**.

Examples

Display GARP timers on port GigabitEthernet 2/0/1.

```
<Sysname> display garp timer interface GigabitEthernet 2/0/1
        GARP timers on port GigabitEthernet2/0/1

                Garp Join Time          : 20 centiseconds
                Garp Leave Time         : 60 centiseconds
                Garp LeaveAll Time      : 1000 centiseconds
                Garp Hold Time          : 10 centiseconds
```

garp timer

Syntax

garp timer { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

View

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

Default Level

2: System level

Parameters

hold: Sets the hold timer.

join: Sets the join timer.

leave: Sets the leave timer.

timer-value: Timer setting (in centiseconds), which must be a multiple of 5.

Description

Use the **garp timer** command to set a GARP timer for an Ethernet port or all ports in a port group in compliance with the timer setting dependencies shown in Table 1-1.

Use the **undo garp timer** command to restore the default of a GARP timer. This may fail if the default does not satisfy the dependencies shown in Table 1-1.

By default, the hold timer, the join timer, and the leave timer are set to 10 centiseconds, 20 centiseconds, and 60 centiseconds.

Note that:

- In Ethernet/Layer-2 aggregate interface view, these two commands apply to the current port only; in port group view, these two commands apply to all the ports in the port group.
- The GVRP configuration made on a link aggregation member port can take effect only after the port is removed from the group. For more information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- When restoring the default GARP timers, you are recommended to do that on the timers in the order of hold, join, leave, and leaveall.
- When configuring GARP timers, note that their values are dependent on each other and must be a multiplier of five centiseconds. If the value range for a timer is not desired, you may change it by tuning the value of another timer as shown in the following table:

Table 1-1 Dependencies of GARP timers

Timer	Lower limit	Upper limit
Hold	10 centiseconds	Not greater than half of the join timer setting
Join	Not less than two times the hold timer setting	Less than half of the leave timer setting
Leave	Greater than two times the join timer setting	Less than the leaveall timer setting
Leaveall	Greater than the leave timer setting	32765 centiseconds

Related commands: **display garp timer**.

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 2/0/1
[Sysname-GigabitEthernet2/0/1] garp timer join 25
```

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 the range 65 to 32765 (in centiseconds), Note that the setting of the leaveall timer must be a multiple of 5 centiseconds and must be greater than the leave timer settings of all the ports.

Description

Use the **garp timer leaveall** command to set the leaveall timer of GARP.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is less than the setting of the current leave timer.

By default, the setting of the leaveall timer is 1000 centiseconds (that is, 10 seconds).

A leaveall timer starts upon the start of a GARP application entity. When this timer expires, the entity sends a LeaveAll message so that other entities can re-register its attribute information and starts another leaveall timer at the same time.

Each time a device on the network receives a LeaveAll message, it resets its leaveall timer. Therefore, a GARP application entity may send LeaveAll messages at the interval set by its leaveall timer or the leaveall timer on another device on the network, whichever is smaller.

Related commands: **display garp timer**.

Examples

Set the leaveall timer to 100 centiseconds, assuming that the leave timer is 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 100
```

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*.

Description

Use the **reset garp statistics** command to clear the GARP statistics of the specified ports or all ports if no ports are specified.

The cleared statistics include the statistics about GVRP packets received, sent and dropped.

Related commands: **display gvrp statistics**.

Examples

Clear statistics about GARP on all ports.

```
<Sysname> reset garp statistics
```

GVRP Configuration Commands

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*: Displays the local VLAN information maintained by GVRP on the port specified 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 2/0/1.

```
<Sysname> display gvrp local-vlan interface GigabitEthernet 2/0/1
 Following VLANs exist in GVRP local database:
  1(default),2-500
```

// The information above shows that GVRP maintains the information about VLAN 1, VLAN 2 through VLAN 500, which GigabitEthernet 2/0/1 belongs to.

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 1, which GigabitEthernet 2/0/1 belongs to.

```
<Sysname> display gvrp state interface GigabitEthernet 2/0/1 vlan 1
        GVRP state of VLAN 1 on port GigabitEthernet2/0/1

                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.

Note that if the **interface** *interface-list* is not provided, the GVRP statistics of all trunk ports will be displayed. Otherwise, only the GVRP statistics of all the specified trunk port will be displayed.

Examples

Display statistics about GVRP for trunk port GigabitEthernet 2/0/1.

```
<Sysname> display gvrp statistics interface GigabitEthernet 2/0/1
        GVRP statistics on port GigabitEthernet2/0/1

                GVRP Status                     : Enabled
                GVRP Running                    : YES
                GVRP Failed Registrations       : 0
                GVRP Last Pdu Origin            : 0000-0000-0000
                GVRP Registration Type          : Normal
```

Table 1-2 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*: Displays the information about dynamic VLAN operations on the port specified 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 2/0/1.

```
<Sysname> display gvrp vlan-operation interface GigabitEthernet 2/0/1
        Dynamic VLAN operations on port GigabitEthernet2/0/1

                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
```

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 the command is executed.

By default, GVRP is disabled.

Note that:

- To enable GVRP on a port, you need to enable it globally first.
- The port where you enable/disable GVRP must be a trunk port.
- GVRP is mutually exclusive with service loopback.
- In an MSTP network, GVRP can run on only the CIST. In addition, blocked ports on the CIST cannot receive/send GVRP packets.
- Enabling GVRP on a Layer-2 aggregate interface enables both the aggregate interface and all selected member ports in the corresponding link aggregation group to participate in dynamic VLAN registration and deregistration. In addition, the GVRP configuration made on a link aggregation member port can take effect only after the port is removed from the group. For more information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

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.

GVRP provides the following three registration types on a port:

- Normal — Enables the port to dynamically register/deregister VLANs, and to propagate both dynamic and static VLAN information.
- Fixed — Disables the port from dynamically registering/deregistering VLANs or propagating information about dynamic VLANs, but allows the port to propagate information about static VLANs. A trunk port with fixed registration type thus allows only manually configured VLANs to pass through even though it is configured to carry all VLANs.
- Forbidden — Disables the port from dynamically registering/deregistering VLANs or propagating VLAN information except information about VLAN 1. A trunk port with forbidden registration type thus allows only VLAN 1 to pass through even though it is configured to carry all VLANs.

Note that:

- This command is only available on trunk ports.
- The GVRP configuration type configuration made on a link aggregation member port can take effect only after the port is removed from the group. For more information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **display garp statistics**.

Examples

Set the GVRP registration type to **fixed** on port GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] gvrp registration fixed
```

Table of Contents

1 QinQ Configuration Commands

QinQ 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 a class, a string of 1 to 31 characters.

behavior-name: Name of a traffic behavior, a string of 1 to 31 characters.

Description

Use the **classifier behavior** command to associate a traffic behavior with a class.

Use the **undo classifier** command to remove the association.

Note that each class can be associated with only one traffic behavior.

Related commands: **qos policy**.

Note

In a QoS policy with multiple class-to-traffic-behavior associations, if the action of creating an outer VLAN tag is configured in a traffic behavior, we recommend you not to configure any other action in this traffic behavior. Otherwise, the QoS policy may not function as expected after it is applied.

Examples

Associate the behavior **test** with the class **database** in the policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

if-match customer-vlan-id

Syntax

if-match customer-vlan-id *vlan-id-list*

undo if-match customer-vlan-id *vlan-id-list*

View

Class view

Default Level

2: System level

Parameters

vlan-id-list: Customer VLAN IDs. You can specify up to eight VLAN IDs for the argument in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous space-separated VLAN IDs. A VLAN ID ranges from 1 to 4094.

Description

Use the **if-match customer-vlan-id** command to use the specified customer VLAN ID(s) as the match criterion.

Use the **undo if-match customer-vlan-id** command to remove the match criterion.

Example

Create class **class1** and classify frames of customer VLAN 9 through 100 to class 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 9 to 100
```

nest top-most vlan-id

Syntax

nest top-most vlan-id *vlan-id*

undo nest

View

Traffic behavior view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094.

Description

Use the **nest top-most vlan-id** command to configure the action of creating an outer VLAN tag for the traffic behavior.

Use the **undo nest** command to remove the action.

Related commands: **qos policy**, **traffic behavior**.

Examples

Configure the action of creating outer VLAN tag 100 for the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] nest top-most vlan-id 100
```

qinq enable

Syntax

qinq enable

undo qinq enable

View

Ethernet port 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 for the current Ethernet port.

Use the **undo qinq enable** command to disable basic QinQ for the current Ethernet port.

By default, basic QinQ is disabled for Ethernet port.

After basic QinQ is enabled on the port, frames on this port will be tagged with a new VLAN tag, the VLAN ID in which is the default VLAN ID of the port.

Configured in Ethernet port view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples

Enable basic QinQ on port GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qinq enable
```

Enable basic QinQ on Layer-2 aggregate interface 1.

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

qinq ethernet-type customer-tag

Syntax

qinq ethernet-type customer-tag *hex-value*

undo qinq ethernet-type customer-tag

View

System view

Default Level

2: System level

Parameters

hex-value: Hexadecimal protocol type ID, in the range of 0x0001 to 0xFFFF, but you cannot set it to any of the protocol type values listed in Table 1-1.

Table 1-1 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 customer-tag** command to configure the TPID value of the customer network VLAN tags.

Use the **undo qinq ethernet-type customer-tag** command to restore the system default.

By default, the TPID value of the customer network VLAN tags is 0x8100.

Examples

Set the TPID value of the customer network VLAN tags to 0x9100.

```
<Sysname> system-view
[Sysname] qinq ethernet-type customer-tag 9100
```

qinq ethernet-type service-tag

Syntax

qinq ethernet-type service-tag *hex-value*

undo qinq ethernet-type service-tag

View

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

Default Level

2: System level

Parameters

hex-value: Hexadecimal protocol type ID, in the range of 0x0001 to 0xFFFF except the protocol type values listed in Table 1-1.

Description

Use the **qinq ethernet-type service-tag** command to configure the TPID value of the service provider network VLAN tags.

Use the **undo qinq ethernet-type service-tag** command to restore the default.

By default, the TPID value of the service provider network VLAN tags is 0x8100.

Examples

Set the TPID value of the service provider network VLAN tags to 0x9100 for GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet2/0/1
[Sysname-GigabitEthernet2/0/1] qinq ethernet-type service-tag 9100
```

qos apply policy

Syntax

qos apply policy *policy-name* **inbound**

undo qos apply policy inbound

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

inbound: Applies the specified policy to the traffic received on the current port(s).

policy-name: Policy name, a string of 1 to 31 characters.

Description

Use the **qos apply policy** command to apply a 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.

In selective QinQ implementation on SC/SA/EA series boards, a QoS policy can be applied only to incoming traffic. Therefore, the **qos apply policy** command can be applied only on ports receiving traffic from the customer network.

Note

For complete information about board types, refer to the accompanied installation manual.

Examples

Apply the policy **test** in the inbound direction of GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos apply policy test inbound
```

qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view

Default Level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 31 characters.

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 has been applied on a port, remove it from the port first.

Related commands: **classifier behavior**, **qos apply policy**.

Examples

Create the policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default Level

2: System level

Parameters

behavior-name: Behavior name, a string of 1 to 31 characters.

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

Create a traffic behavior **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

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 between the match criteria in the specified class as logical AND. That is, a packet belongs to the class only when it matches all the match criteria defined in the class.

or: Specifies the relationship between the match criteria in the class as logical OR. That is, a packet belongs to the class if it matches a match criterion defined in the class.

classifier-name: Class name, a string of 1 to 31 characters.

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 belongs to the class only when it matches all match criteria defined in the class.

Examples

Create the class **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Table of Contents

1 BPDU Tunneling Configuration Commands

BPDU Tunneling Configuration Commands

bpdu-tunnel dot1q stp

Syntax

bpdu-tunnel dot1q stp

undo bpdu-tunnel dot1q stp

View

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

Default Level

2: System level

Parameters

None

Description

Use the **bpdu-tunnel dot1q stp** command to enable BPDU tunneling for STP on the current port or ports.

Use the **undo bpdu-tunnel dot1q stp** command to disable BPDU tunneling for STP on the port or ports.

By default, BPDU tunneling for STP is disabled.

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 only on the Layer-2 aggregate interface. Configuration made in port group view takes effect on all ports in the port group.
- Configuration made on an aggregation group member port takes effect after the port exits the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- Before you can enable BPDU tunneling for STP on a port, disable STP on the port first.

Examples

Enable BPDU tunneling for STP on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp disable
[Sysname-GigabitEthernet2/0/1] bpdu-tunnel dot1q stp
```

Enable BPDU tunneling for STP on all the ports in port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member GigabitEthernet 2/0/1 to gigabitethernet 2/0/6
[Sysname-port-group-manual-1] stp disable
[Sysname-port-group-manual-1] 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 BPDU tunnel frames, in the format of H-H-H. The allowed values are 0100-0CCD-CDD0, 0100-0CCD-CDD1, 0100-0CCD-CDD2, and 010F-E200-0003.

Description

Use the **bpdu-tunnel tunnel-dmac** command to configure the destination multicast MAC address for BPDU tunnel frames.

Use the **undo bpdu-tunnel tunnel-dmac** command to restore the default value.

By default, the destination multicast MAC address for BPDU tunnel frames is 0x010F-E200-0003.

Examples

Set the destination multicast MAC address for BPDU tunnel frames to 0100-0CCD-CDD0.

```
<Sysname> system-view
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

Table of Contents

1 VLAN Mapping Configuration Commands

Note

- On the S7900E series switches, VLAN mapping is achieved mainly through QoS policies. This chapter introduces part of the commands for ports involved in many-to-one VLAN mapping. For QoS policy configuration commands, refer to *QoS Commands* in the *QoS Volume*.
- Only SC boards support many-to-one VLAN mapping. For detailed introduction to boards, refer to the *Installation Manual*.

VLAN Mapping Configuration Commands

qinq enable downlink

Syntax

qinq enable downlink

undo qinq enable

View

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

Default Level

2: System level

Parameters

None

Description

Use the **qinq enable downlink** command to enable customer-side QinQ on the current Ethernet port(s).

Use the **undo enable downlink** command to disable customer-side QinQ on the current Ethernet port(s).

By default, customer-side QinQ is disabled on Ethernet ports.

Configuration made in Ethernet interface view takes effect on the current port only, while configuration made in port group view takes effect on all ports in the port group.

Examples

Enable customer-side QinQ on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qinq enable downlink
```

Enable customer-side QinQ on port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 2/0/1 to gigabitethernet 2/0/6
[Sysname-port-group-manual-1] qinq enable downlink
```

qinq enable uplink

Syntax

qinq enable uplink

undo qinq enable

View

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

Default Level

2: System level

Parameters

None

Description

Use the **qinq enable uplink** command to enable service provider-side QinQ on the current Ethernet port(s).

Use the **undo enable downlink** command to disable service provider-side QinQ on the current Ethernet port(s).

By default, service provider-side QinQ is disabled on Ethernet ports.

Configuration made in Ethernet interface view takes effect on the current port only, while configuration made in port group view takes effect on all ports in the port group.

Examples

Enable service provider-side QinQ on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qinq enable uplink
```

Enable service provider-side QinQ on port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 2/0/1 to gigabitethernet 2/0/6
[Sysname-port-group-manual-1] qinq enable uplink
```

Table of Contents

1 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 local Ethernet OAM connection information.

```
<Sysname> display oam local
Port        : GigabitEthernet2/0/1
Link Status : Up
EnableStatus              : Enable
Local_oam_mode            : Active      Local_pdu             : ANY
Local_mux_action          : FWD         Local_par_action      : DISCARD
Port        : Ethernet1/2
Link Status : Down
EnableStatus              : Enable
Local_oam_mode            : Active      Local_pdu             : LF_INFO
Local_mux_action          : FWD         Local_par_action      : FWD
```

Table 1-1 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 Ethernet OAMPDUs of different types are processed locally. This field can be: • RX_INFO, indicating the port only receives Information OAMPDUs and does not send 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 only sends and receives Information OAMPDUs • ANY, indicating the port sends and receives Ethernet OAMPDUs of any types
Local_mux_action	Local sending mode, which can be: • FWD, indicating the port can send any packets • DISCARD, indicating the port only sends Ethernet OAMPDUs
Local_par_action	Local receiving mode, 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.

Display the information about the Ethernet OAM connection established on the local port GigabitEthernet 2/0/1.

```
<Sysname> display oam local interface GigabitEthernet 2/0/1
Port        : GigabitEthernet2/0/1
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 1-2 display oam local interface 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. Refer to Table 1-1 for more.
Local_pdu	The way in which Ethernet OAMPDUs of different types are processed locally. Refer to Table 1-1 for more.
Local_mux_action	Local sending mode. Refer to Table 1-1 for more.
Local_par_action	Local receiving mode. Refer to Table 1-1 for more.
OAMLocalFlagsField	Local flags inserted in the local flag fields of the Ethernet OAMPDUs sent
Link Fault	Indicates whether Ethernet OAM link error events occurred. A value of 0 indicates no Ethernet OAM error event occurs; a value of 1 indicates Ethernet OAM error event occurrences.
Dying Gasp	Indicate whether Dying Gasp events occurred. A value of 0 indicates no Dying Gasp event occurs; a value of 1 indicates Dying Gasp event occurrences.
Critical Event	Indicates whether Critical Events occurred. A value of 0 indicates no Critical event occurs; a value of 1 indicates Critical event occurrences.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete.
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete.
Packets statistic	Statistics on 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 peer Ethernet OAM connection information.

```
<Sysname> display oam remote
Port        :GigabitEthernet2/0/1
Link Status :Up
Information of the latest received OAM packet:
```

```
OAMRemoteMACAddress       : 00e0fc003552
OAMRemotePDUConfiguration : 1500
Remote_mux_action         : FWD         Remote_par_action      : FWD
```

Table 1-3 display oam remote 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
Remote_mux_action	Peer sending mode. Refer to Table 1-1 for more.
Remote_par_action	Peer receiving mode. Refer to Table 1-1 for more.

Display the Ethernet OAM information about the peer port GigabitEthernet 2/0/1.

```
<Sysname> display oam remote interface GigabitEthernet 2/0/1
Port        : GigabitEthernet2/0/1
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 1-4 display oam remote interface command output description

Field	Description
Port	Port index
Link Status	Link status

Field	Description
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 1-1 for more.
Remote_par_action	Peer receiving mode. Refer to Table 1-1 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 Ethernet OAM link error events occurred. Refer to Table 1-2 for more.
Dying Gasp	Indicate whether Dying Gasp events occurred. Refer to Table 1-2 for more.
Critical Event	Indicate whether Critical events occurred. Refer to Table 1-2 for more.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete.
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete.

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-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 1-5 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.
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*: Specifies 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        : GigabitEthernet2/0/1
Link Status : Up
Event statistic :
------------------------------------------------------------------------
Link Fault    :0    Dying Gasp    : 0    Critical Event    : 0
```

Table 1-6 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 Ethernet OAM link error events occurred. Refer to Table 1-2 for more.
Dying Gasp	Indicates whether Dying Gasp events occurred. Refer to Table 1-2 for more.
Critical Event	Indicates whether Critical events occurred. Refer to Table 1-2 for more.

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*: Specifies 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**.

Examples

Display the statistics on Ethernet OAM link error events occurred on all the local ports.

```
<Sysname> display oam link-event local
Port        : GigabitEthernet2/0/1
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 1-7 display oam link-event local command output description

Field	Description
Port	Port index
Link Status	Link status
OAMLocalErrFrameEvent : (ms = milliseconds)	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 error 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.

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 an 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.

After you enable Ethernet OAM for an Ethernet port, the port attempts to establish an OAM connection to the peer in the predetermined mode.

Related commands: **oam mode**.

Examples

Enable OAM on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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.

An error frame event occurs when a errored frame detection interval expires and the number of the frame errors occurred on an Ethernet port is larger than (or equal to) the errored frame event triggering threshold.

The errored frame detection interval applies to all the Ethernet ports on which OAM connections are established.

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.

An errored frame event occurs when a errored frame detection interval expires and the number of the frame errors occurred on an Ethernet port is larger than (or equal to) the errored frame event triggering threshold.

The errored frame event triggering threshold configured applies to all the Ethernet ports on which Ethernet OAM connections are established.

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 60,000 (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).

A errored frame period event occurs when a errored frame period detection interval expires and the number of the frame errors occurred on an Ethernet port is larger than (or equal to) the errored frame period event triggering threshold.

The errored frame period detection interval configured applies to all the Ethernet ports on which OAM connections are established.

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.

```
<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.

A errored frame period event occurs when a errored frame period detection interval expires and the number of the frame errors occurred on an Ethernet port is larger than (or equal to) the errored frame period event triggering threshold.

The errored frame period event triggering threshold configured applies to all the Ethernet ports on which OAM connections are established.

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.

A errored frame seconds event occurs when a errored frame seconds detection interval expires and the number of the error seconds of an Ethernet port is larger than (or equal to) the errored frame seconds event triggering threshold. (A second is called an error second if error frames occur in the second.)

The errored frame seconds detection interval configured applies to all the Ethernet ports on which Ethernet OAM connections are established.

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.

A errored frame seconds event occurs when a errored frame seconds detection interval expires and the number of the error seconds of an Ethernet port is larger than (or equal to) the errored frame seconds event triggering threshold. (A second is called an error second if error frames occur in the second.)

The errored frame seconds event triggering threshold configured applies to all the Ethernet ports on which Ethernet OAM connections are established.

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 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 loopback testing.

By default, Ethernet OAM loopback testing is disabled.

Note that:

- Ethernet OAM loopback testing is available only after the Ethernet OAM connection is established.
- Ethernet OAM loopback testing can be performed by Ethernet OAM entities operating in the active Ethernet OAM mode only.
- Ethernet OAM loopback testing is available only when it is supported on both the local port and the peer port.
- Enabling Ethernet OAM loopback testing interrupts data communications. After Ethernet OAM loopback testing is disabled, all the ports involved will be shut down and then brought up.
- Ethernet OAM loopback testing is disabled when you execute the **undo oam enable** command to disable Ethernet OAM, when you execute the **undo oam loopback** command to disable Ethernet OAM loopback testing, or when the Ethernet OAM connection is timed out.

Related commands: **oam enable**, **oam mode**.

Examples

Enable Ethernet OAM loopback testing on GigabitEthernet2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] oam mode active
[Sysname-GigabitEthernet2/0/1] oam enable
[Sysname-GigabitEthernet2/0/1] 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:

- No Ethernet OAM connection can be established between two Ethernet ports operating in the passive Ethernet OAM mode.
- For an Ethernet OAM-enabled Ethernet port, the Ethernet OAM operating mode cannot be changed. To do this, you need to disable Ethernet OAM on the port first.

Related commands: **oam enable**.

Examples

Configure GigabitEthernet 2/0/1 to operate in the active Ethernet OAM mode.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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*: Specifies 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
```

Table of Contents

1 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 interface 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 2/0/1, Enable CCM sending on service point 3.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 5 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 5 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 1-1.

Table 1-1 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
5	1 second	3.5 seconds
6	10 seconds	35 seconds
7	60 seconds	210 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
```

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 1-2 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	• 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
```

cfd loopback

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *loopback-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 *loopback-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 1-3 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.

```
<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-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.

```
<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 interface view

Default level

2: System level

Parameters

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 a MEP.

```
<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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 interface 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.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 1-4 to create or not create MIPs (within a single VLAN):

Table 1-4 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 interface 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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

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 a service instance.

```
<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 1-5 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 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.

Field	Description
Relay Action	• 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.

These LTR messages are stored in the buffer after you executed the **cfd linktrace auto-detection** command. With the **size** parameter not specified, this command will display the information of all LTRs stored in the buffer.

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: 255
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: 255
MAC Address               TTL        Forwarded        Relay Action
00E0-FC27-6502            63         No                    None
```

Table 1-6 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	• 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
2 maintenance association(s) belong(s) to maintenance domain mdtest_6:
Maintenance association: matest_6
Service instance: 6          VLAN: 6          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 1-7 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 1-8 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 a MEP.

```
<Sysname> display cfd mep 50 service-instance 1
Interface: GigabitEthernet2/0/2
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 are received. The last-received CCM:
Maintenance domain: mdtest1
Maintenance association: matest1
MEP ID: 5       Sequence Number: 0x34fc
MAC Address: 0000-FC00-6504
Received Time: 2008/05/06 16:33:09

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 0000-FC00-6503
Received Time: 2008/05/06 16:33:15

Some other MEPs are transmitting the RDI bit.
```

Table 1-9 display cfd mep command output description

Field	Description
Interface	Interface that an MD belongs to
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

Field	Description
FNG state	State of FNG (Fault Notification Generator), including: FNG_RESET, FNG_DEFECT, FNG_REPORT_DEFECT, FNG_DEFECT_REPORTED, FNG_DEFECT_CLEARING
CCM	Information related to CCM
Current state	State of CCMs sent, including: 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 device
Received Time	Time when the last error CCM is received
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.

If no port is specified, this command will display the MP information of all ports.

The information displayed is ordered by port name primarily, and within a single port, ordered by VLAN ID (from small to big), and within a single VLAN, in the order of outward-facing MEPs (from low to high level), MIPs, and inward-facing MEPs (from high to low level).

Examples

Display the MP information.

```
<Sysname> display cfd mp
Interface GigabitEthernet2/0/2   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 GigabitEthernet2/0/4   VLAN 1
MEP ID: 9        Level: 6    Service instance: 6      Direction: Outbound
Maintenance domain: mdtest6
Maintenance association: matest6
```

Table 1-10 display cfd mp command output description

Field	Description
Interface GigabitEthernet2/0/2 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 the remote MEP.

```
<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 1-11 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: GigabitEthernet2/0/1               Direction: Inbound
```

Table 1-12 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.
```

Table of Contents

1 OLT Configuration Commands

Note

- This document discusses the commands specific to Ethernet Passive Optical Network (EPON). For the commands of switch features on optical line terminal (OLT) and optical network unit (ONU) ports, refer to 4 Switch Feature-Related Configuration Commands.
- The actual output information varies with devices.

OLT Configuration Commands

dba-algorithm enable

Syntax

dba-algorithm enable { **extdba** | **intdba** }

undo dba-algorithm update

View

OLT port view

Default Level

2: System level

Parameters

extdba: Enables the external DBA algorithm for implementation through an external DBA algorithm file.

intdba: Enables the internal DBA algorithm for implementation within the device.

Description

Use the **dba-algorithm enable** command to enable the internal or external DBA algorithm.

Use the **undo dba-algorithm update** command to remove the loaded external DBA algorithm file and restore the internal DBA algorithm.

By default, the internal DBA algorithm is enabled.

To use the **dba-algorithm enable** command to enable the external DBA algorithm, use the **dba-algorithm update** command to load the specified DBA algorithm file first.

Caution

- When you use the **dba-algorithm update** command to upgrade the external DBA algorithm, the new upgrade file is synchronously loaded onto the backup SRPU, and overwrites the old one (if any) in the backup SRPU. If the synchronous upgrading operation fails (this may occur when there is not enough free space on the Flash of the backup SRPU), DBA algorithms on the primary and backup SRPUs will be different, thus resulting in configuration errors.
- To avoid service interruption, enable a new DBA algorithm when no service is in progress.

Examples

Load an external DBA algorithm file plato2.app.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] dba-algorithm update plato2.app
 Updating external DBA-algorithm.......
```

Enable the external DBA algorithm. Enable the external DBA algorithm.

```
[Sysname-Olt3/0/1] dba-algorithm enable extdba
```

dba-algorithm update

Syntax

dba-algorithm update *file-url*

View

OLT port view

Default Level

2: System level

Parameters

file-url: String of up to 64 characters consisting of device name and the filename of the DBA algorithm. If no device name is entered, the Flash of the switching and routing process unit (SRPU) will be used. Moreover, the DBA algorithm file on the backup SRPU cannot be used for the upgrade.

Description

Use the **dba-algorithm update** command to load the specified external DBA algorithm file.

Examples

Load the external DBA algorithm file plato2.app.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] dba-algorithm update plato2.app
 Updating external DBA-algorithm.......
```

dba-parameters

Syntax

dba-parameters { **discovery-frequency** *value* | **discovery-length** *value* | **cycle-length** *value* } *

undo dba-parameters { **discovery-frequency** | **discovery-length** | **cycle-length** } *

View

OLT port view

Default Level

2: System level

Parameters

discovery-frequency *value*: Specifies the cycle for the OLT to send discovery GATE frames (the cycle is known as grant cycle, which is measured in cycle-length). The *value* argument ranges from 25 to 100, and defaults to 50 if you do not use the **discovery-frequency** keyword (that is, the OLT sends discovery GATE frames every 50 cycle-lengths).

discovery-length *value*: Specifies the period in TQs for the OLT to discover ONUs. The *value* argument ranges from 21845 to 87381 and defaults to 41500.

cycle-length *value*: Specifies the cycle-length in TQs (cycle-length is the measurement unit of grant cycle). The *value* argument ranges from 32768 to 131070; it defaults to 65535 if you do not use the **cycle-length** keyword.

Note

1 time quantum (TQ) is equal to 16 ns, which is the time it takes to transmit two bytes of data at 1 Gbps.

Description

Use the **dba-parameters** command to specify the cycle for the OLT to send discovery frames to ONUs and the period in TQs for the OLT to discover ONUs.

Use the **undo dba-parameters** command to restore the default DBA parameter values.

Use the two commands only when necessary.

Examples

Configure OLT 3/0/1 to periodically send discovery GATE frames at the interval of 30 cycle-lengths.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] dba-parameters discovery-frequency 30
```

display epon-capability interface

Syntax

display epon-capability interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT** or **ONU**.

interface-number: OLT/ONU port number.

Note

- As for the *interface-number* argument, the format of LPU slot number/sub-LPU slot number/OLT port number is used for OLT ports; and the format of LPU slot number/sub-LPU slot number/OLT port number:ONU port number is used for ONU ports.
- To create an ONU port, use the **using onu** command in OLT port view.

Description

Use the **display epon-capability interface** command to display OLT or ONU capability information.

- If interface-type interface-number identifies an OLT port, the following information about the OLT is displayed: automatic gain control (AGC) time and clock data recovery (CDR) time.
- If interface-type interface-number identifies an ONU port, the following information about the ONU is displayed: laser on time, laser off time, and grant FIFO deep.

Caution

- Before displaying the version information about an ONU, make sure the ONU is bound and is in Up state (that is, the ONU is online). Refer to the **bind onuid** command for more.
- Before displaying the version information about an OLT, make sure the OLT is in Up state.

Note

- Because location distance and external conditions of each ONU are different, the received signal maybe strong or weak. AGC time is the time used by the OLT to automatically restore the strength of the received signal to an acceptable level.
- CDR time is the time used by the OLT to synchronize the phase and frequency of received signals.
- ONU laser on time is the interval between when the ONU laser is turned on and when it becomes stable. ONU laser off time is the interval between when the ONU laser is turned off and when it becomes stable.

Examples

Display OLT capability information.

```
<Sysname> display epon-capability interface olt 3/0/1
 OLT device capability information:
 AGC lock time(TQ): 14
 CDR lock time(TQ): 20
```

Display ONU capability information.

```
<Sysname> display epon-capability interface onu 3/0/1:1
 ONU device capability information:
 Laser on time(TQ) : 32
 Laser off time(TQ): 32
 Grant FIFO deep   : 8
```

Table 1-1 display epon-capability interface command output description

Field	Description
AGC lock time(TQ): 14	AGC time, in TQ
CDR lock time(TQ): 20	Clock data recovery time, in TQ
Grant FIFO deep : 8	Grant queue depth, namely, size of the FIFO queue (measured by the number of timeslots)

display epon-oam interface

Syntax

display epon-oam interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type. It is ONU.

interface-number: ONU port number.

Description

Use the **display epon-oam interface** command to display the operation, administration, and maintenance (OAM) information about an ONU.

To display the OAM information about an ONU, make sure the ONU is online.

Examples

Display the OAM information about an ONU.

```
<Sysname> display epon-oam interface onu 3/0/1:1
 OAM information:
```

```
OAM version: 3.3
Multiplexer action: forwarding non-OAM PDUs to the lower sublayer
Parser action     : forwarding non-OAM PDUs to higher layer
Organization specific information TLVs: support
Organization specific events          : support
Organization specific OAM PDUs        : support
Sending variable response OAM PDUs    : support
Interpreting link events              : not support
OAM mode              : passive
Unidirectional support: disable
Loopback support      : enable
Maximal PDU size(byte): 1518
Enterprise number     : 1111
Device identifier     : 6301
Version identifier    : 0
Board vendor code     : 0
Board model identifier: 0
```

Table 1-2 display epon-oam interface command output description

Field	Description
Multiplexer action: forwarding non-OAM PDUs to the lower sublayer	The action of the multiplexer: Forwarding non-OAM PDUs to the lower layer
Parser action: forwarding non-OAM PDUs to higher layer	The action of the parser: Forwarding non-OAM PDUs to the higher layer
Organization specific information TLVs	This field indicates whether or not the OAM version supports TLV-format organization specific information.
Organization specific events	This field indicates whether or not the OAM version supports organization specific events.
Organization specific OAM PDUs	This field indicates whether or not the OAM version supports organization specific OAM PDUs.
Sending variable response OAM PDUs	This field indicates whether or not the OAM version supports the sending of variables through response OAM PDUs.
Interpreting link events	This field indicates whether or not the OAM version supports the interpreting of link events.
Unidirectional support	Unidirectional support mode
Loopback support	Loopback support mode
Maximal PDU size(byte)	Maximum PDU size (in bytes)
Enterprise number	Enterprise identifier

display epon-parameter slot

Syntax

display epon-parameter slot *slot-number*

View

Any view

Default Level

1: Monitor level

Parameters

slot-number: Slot number of the EPON service board.

Description

Use the **display epon-parameter slot** command to display related information of EPON parameters, such as message timeout time in extended OAM discovery, OUI and extended OAM version number list, and encrypted parameters.

Related commands: **epon-parameter ouilist**, **encryption timer**.

Examples

Display related information of EPON parameters

```
<Sysname> display epon-parameter slot 3
 Parameters:
     oui: 111111     oam-version: 1 (default)
     oui: 111111     oam-version: 2
 encryption-timing :
     update-key-time : 10s
     no-reply-timeout : 3.0s
 eoam-discovery-timeout : 3.0s
```

Table 1-3 display epon-parameter command output description

Field	Description
Parameters	EPON system parameters
oui: 111111 oam-version: 1 (default)	The default Organizationally Unique Identifier (OUI) of EPON service board(s) and the extended OAM version
oui: 111111 oam-version: 2	The user-defined OUI and the extended OAM version
encryption-timing :	Encryption time
update-key-time : 10s	Key update interval, in seconds
no-reply-timeout : 3.0s	Encryption response timeout time, in seconds
eoam-discovery-timeout : 3.0s	Extended OAM discovery timeout time, in seconds

display epon-version interface

Syntax

display epon-version interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT** or **ONU**.

interface-number: OLT/ONU port number.

Description

Use the **display epon-version interface** command to display OLT or ONU version information.

- Before displaying the version information about an ONU, make sure the ONU is online.
- Before displaying the version information about an OLT, make sure the OLT port is in Up state.

Examples

Display OLT version information.

```
<Sysname> display epon-version interface olt 3/0/1
 OLT device version information:
 Firmware major version: 5
 Firmware minor version: 1
 Hardware major version: 5201
 Hardware minor version: 1
 Supported LLID number : 127
```

Display ONU version information.

```
<Sysname> display epon-version interface onu 3/0/1:1
 ONU device version information:
 Hardware major version: 6301
 Hardware minor version: 0
 Supported LLID number : 1
 MAC type of UNI port  : GMII
```

Table 1-4 display epon-version command output description

Field	Description
Supported LLID number	Number of supported LLIDs
MAC type of UNI port	MAC type of a user network interface (UNI) port: • Gigabit Media Independent Interface (GMII) • Media Independent Interface (MII)

Note

A Logical Link Identifier (LLID) uniquely identifies an ONU. It is dynamically allocated by an OLT.

display epon-workmode interface

Syntax

display epon-workmode interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT** or **ONU**.

interface-number: OLT/ONU port number.

Description

Use the **display epon-workmode interface** command to display the current work mode of an OLT or ONU. If the port type is OLT, this command can also display its MAC address and dynamic bandwidth allocation (DBA) algorithm mode.

To display the working mode of an ONU, make sure the ONU is online.

Table 1-5 Work status and description

Item	Status	Description
OLT	open	The OLT is open.
	closed	The OLT is closed.
ONU	open	The ONU is open.
	closed	The ONU is closed.
DBA algorithm mode	internal	Internal DBA algorithm
	external	External DBA algorithm

Examples

Display the OLT working mode.

```
<Sysname> display epon-workmode interface olt 3/0/1
 OLT work mode:
 Status  : open
 MAC ADDR: 000f-e2a1-1027
 DBA mode: internal
```

Display the ONU working mode.

```
<Sysname> display epon-workmode interface onu 3/0/1:1
 ONU work mode:
 Working status: open
 FEC mode : disable
```

Table 1-6 display epon-workmode command output description

Field	Description
Status: open	The OLT is open.
MAC ADDR: 000f-e2a1-1027	The MAC address the OLT resides is 000f-e2a1-1027. All the OLT ports under a switch use the same MAC address.
DBA mode: internal	Internal DBA algorithm is adopted.
Working status: open	The ONU is open.
FEC mode : disable	FEC is disabled

display epon statistics interface

Syntax

display epon statistics interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT** or **ONU**.

interface-number: OLT/ONU port number.

Description

Use the **display epon statistics interface** command to display the statistics on a specified ONU/OLT port, including average error rate of data bits or data frames of the data exchanged between the OLT and the ONUs.

Note

- To display the statistics of an OLT, make sure the OLT is up.
- To display the statistics of an ONU, make sure the ONU is online.
- This command displays the average error rate, instead of the accumulated error rate, within a sampling interval. An error rate value less than 1e-9 is displayed as **0**.

Examples

Display the statistics of an OLT port.

```
<Sysname> display epon statistics interface olt 3/0/1
 OLT statistics:
 PON Bit error rate(in 1e-9 unit): 0
 CNI Bit error rate(in 1e-9 unit): 0
```

Display the statistics of an ONU port.

```
<Sysname> display epon statistics interface onu 3/0/1:1
 ONU statistics:
 Bit error rate(in 1e-9 unit)  : 0
 Frame error rate(in 1e-9 unit): 0
```

Table 1-7 display epon statistics interface command output description

Field	Description
PON Bit error rate(in 1e-9 unit)	PON Bit error rate
CNI Bit error rate(in 1e-9 unit)	Core Network Interface (CNI) Bit error rate. The CNI is the interface between the OLT chip and switching chip of the S7900E switch.

display fiber-backup group

Syntax

display fiber-backup group { **all** | *group-number* }

View

Any view

Default Level

2: System level

Parameters

all: Specifies all the fiber backup groups.

group-number: Fiber backup group number, in the range 1 to 80.

Description

Use the **display fiber-backup group** command to display the information of the member OLT ports, their roles and states in the specified or all fiber backup groups.

Examples

Display the information of the member OLT ports, their roles and states in fiber backup group 1.

```
<Sysname> display fiber-backup group 1
 fiber backup group 1 information:
 Member         Role       State
---------------------------------
 Olt3/0/3       MASTER     ACTIVE
 Olt3/0/4       SLAVE      READY
```

Table 1-8 display fiber-backup group command output description

Field	Description
fiber backup group 1 information:	Information about fiber backup group 1
Member	Member port information of the fiber backup group
Role	Role of the OLT port in the backup group: • MASTER: master port • SLAVE: slave port
State	OLT port state: • ACTIVE: The master port is active (the chip is active and the optical module is plugged in). • READY: The slave port is ready and a master-slave switchover can be performed. • DOWN: Any other condition.

display onu-event interface

Syntax

display onu-event interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type. It is ONU.

interface-number: ONU port number.

Description

Use the **display onu-event interface** command to display the registration and deregistration records of an ONU.

Note

- The system supports up to 50 records for each ONU. After the number of records for an ONU reaches this maximum number, the old records will be overwritten by the new ones.
- If an ONU port is unbound from its ONU or the EPON card is reset, records will be cleared.

Examples

Display the registration and deregistration information of the ONU.

```
<Sysname> display onu-event interface onu 3/0/1:1
Date         Time       ONU Event       ONU Status
2007/07/28   13:57:03   Registration    Down
2007/07/28   18:00:06   Deregistration  Up
```

Table 1-9 display onu-event interface command output description

Field	Description
Date	Date of the ONU event
Time	Time of the ONU event
ONU Event	ONU event: • Registration • Deregistration
ONU Status	ONU status when an ONU event occurs: • Up: when the ONU status is up, the ONU is deregistered. • Down: when the ONU status is down, the ONU is registered.

display onuinfo

Syntax

display onuinfo { **interface** *interface-type interface-number* | **slot** *slot-number* }

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT** or **ONU**.

interface-number: OLT/ONU port number.

slot-number: Slot number of the EPON card.

Description

Use the **display onuinfo** command to display the information about all the ONUs under an OLT port, ONU port, or the EPON card in the specified slot.

The displayed information includes ONU MAC address, LLID that OLT assigns to an ONU, actual length of the optical fiber between an OLT and an ONU, bound ONU port number, ONU type, hardware version, software version, EEPROM version, ONU status, and ONU MAC aging time.

Examples

Display the information about all the legal ONUs under OLT 4/0/1 port.

```
<Sysname> display onuinfo interface Olt 4/0/1
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b90     1     <50   Onu4/0/1:2  ET704-A-L/B  110/100      Up    N/A
 000f-e234-5678     0     N/A   Onu4/0/1:1          N/A      N/A Offline    N/A
 000f-e276-4b93     0     N/A          N/A          N/A      N/A  Silent   284s

 ---  3 entries found  ---
```

Display the information about ONU port ONU 4/0/1:2.

```
<Sysname> display onuinfo interface Onu 4/0/1:2
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b93     1     <50   Onu4/0/1:2  ET704-A-L/B  110/100      Up    N/A

 ---  1 entry found  ---
```

Display the information about all the ONUs on the EPON card in slot 4.

```
<Sysname> display onuinfo slot 4
------------------------------- Olt4/0/1 -------------------------------
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b93     1     <50   Onu4/0/1:2  ET704-A-L/B  110/100      Up    N/A
 000f-e234-5678     0     N/A   Onu4/0/1:1          N/A      N/A  Offline   N/A
------------------------------- Olt4/0/2 -------------------------------
 Error: The port's state should be up!
------------------------------- Olt4/0/3 -------------------------------
 Error: The port's state should be up!
------------------------------- Olt4/0/4 -------------------------------
 Error: The port's state should be up!

 ---  2 entries found  ---
```

Table 1-10 display onuinfo command output description

Field	Description
ONU Mac Address	MAC address of the ONU
LLID	Link ID that OLT automatically assigns to a registered ONU. **0** displays if the ONU is not registered.
Dist(M)	Actual length of the optical fiber between the OLT and the ONU. **N/A** displays if the ONU is not registered.

Field	Description
Port	Number of the port to which an ONU is bound. **N/A** displays if the ONU is not bound to any ONU port.
Board/Ver	ONU model and PCB version number. **N/A** displays if the ONU is not registered.
Sft/Eeprom	ONU software version number and EEPROM version number. **N/A** displays if the ONU is not registered.
State	State of an ONU: • **Silent** displays if the ONU is powered on but not bound to an ONU port. • **Offline** displays if the ONU is not powered on but bound to an ONU port. • **Up** displays if the ONU is started up and bound to an ONU port. • **Down** displays if the ONU is bound to an ONU port but is shut down manually.
Aging	MAC address aging time of an ONU in the silent state. **N/A** displays if the ONU is not in the silent state.
Error: The port's state should be up!	The OLT port is not UP.

display onuinfo mac-address

Syntax

display onuinfo mac-address *mac-address*

View

Any view

Default Level

2: System level

Parameters

mac-address: MAC address of the ONU.

Description

Use the **display onuinfo mac-address** command to display the information about the legal ONU with the specified MAC address.

Examples

Display the information about the legal ONU with the specified MAC address.

```
<Sysname> display onuinfo mac-address 000f-e276-4b93
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b93     1     <50   Onu4/0/1:2  ET704-A-L/B  110/100      Up    N/A

---  1 entry found  ---
```

For the command output description, refer to Table 1-10.

display onuinfo silent

Syntax

display onuinfo silent { **interface** *interface-type interface-number* | **slot** *slot-number* }

View

Any view

Default Level

2: System level

Parameters

interface-type: Port type, which can be **OLT**.

interface-number: OLT port number.

slot-number: ID of the slot where the EPON card is seated.

Description

Use the **display onuinfo silent** command to display the information about all the silent ONUs connected to the specified OLT port or to the EPON card seated in the specified slot.

Examples

Display the information about all the silent ONUs connected to the EPON card seated in slot 4.

```
<Sysname> display onuinfo silent slot 4
------------------------------- Olt4/0/1 ------------------------------
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b90     0     N/A          N/A          N/A      N/A  Silent   266s
------------------------------- Olt4/0/2 ------------------------------
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b91     0     N/A          N/A          N/A      N/A  Silent   252s
------------------------------- Olt4/0/3 ------------------------------
 Error: The port's state should be up!
------------------------------- Olt4/0/4 ------------------------------
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b93     0     N/A          N/A          N/A      N/A  Silent   300s


 ---  3 entries found  ---
```

Display the information about all the silent ONUs connected to OLT 4/0/1.

```
<sysname> display onuinfo silent interface Olt 4/0/1
 ONU Mac Address LLID Dist(M)         Port    Board/Ver  Sft/Epm   State  Aging
 000f-e276-4b90     0     N/A          N/A          N/A      N/A  Silent   243s
 ---  1 entry found  ---
```

For the command output description, refer to Table 1-10.

display optics-parameters interface

Syntax

display optics-parameters interface *interface-type interface-number*

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type, which can be **OLT**.

interface-number: OLT port number.

Description

Use the **display optics-parameters interface** command to display the optical parameter information of the OLT port.

Examples

Display the optical parameter information of the OLT port.

```
<Sysname> display optics-parameters interface olt 2/0/8
Configuration source:                     HOST
 AGC lock time:                            14
 EPON AGC gate offset:                     18
 EPON AGC discovery offset:                18
 EPON AGC duration:                        0
 EPON AGC polarity:                        low
 CDR lock time:                            20
 EPON CDR gate offset:                     32
 EPON CDR discovery offset:                32
 EPON CDR duration:                        0
 EPON CDR polarity:                        high
 CDR end of grant gate offset:             36
 CDR end of grant duration:                2
 CDR end of grant polarity:                low
 Optics end of grant gate offset:          36
 Optics end of grant duration:             2
 Optics end of grant polarity:             low
 Discovery re-locking:                     disable
 Laser Rx loss signal polarity:            low
 EPON optics transmission signal polarity: low
 Optics dead zone:                         10
 Use optics signal loss:                   false
 EPON port link indication polarity:       low
 CNI port link indication polarity:        high
 EPON tbc polarity:                        low
```

```
Discovery laser on time:                32
Discovery laser off time:               32
EPON Tx signal:                         enable
```

Table 1-11 display optics-parameters interface command output description

Field	Description
Configuration source: HOST	Source of the optics configuration settings
AGC lock time: 14	PON upstream data AGC lock time, in TQ
EPON AGC gate offset: 18	AGC reset activation offset before normal grant CDR reset activation
EPON AGC discovery offset: 18	AGC reset activation offset before discovery CDR reset activation
EPON AGC duration: 0	Specific duration, or reference mode
EPON AGC polarity: low	AGC reset pulse polarity
CDR lock time: 20	PON Rx signal synchronization time
EPON CDR gate offset: 32	CDR reset activation offset before start of normal grant
EPON CDR discovery offset: 32	CDR reset activation offset before start of discovery window
EPON CDR duration: 0	Specific CDR reset pulse duration, or lock to reference mode
EPON CDR polarity: high	CDR reset pulse polarity
CDR end of grant gate offset: 36	End of grant reset activation offset(CDR)
CDR end of grant duration: 2	End of grant reset pulse duration(CDR)
CDR end of grant polarity: low	End of grant reset pulse polarity(CDR)
Optics end of grant gate offset: 36	End of grant reset activation offset (Optics)
Optics end of grant duration: 2	End of grant reset pulse duration (Optics)
Optics end of grant polarity: low	End of grant reset pulse duration (Optics)
Discovery re-locking: disable	Whether to disable or enable the Rx PHY re-locking mechanism during discovery window
Laser Rx loss signal polarity: low	Laser Rx loss signal polarity
EPON optics transmission signal polarity: low	PON optics transmission signal polarity
Optics dead zone: 10	Minimal length between the end of a grant to the start of the other
Use optics signal loss: false	Whether to use the optics signal loss signal provided by the OLT line status state machine: false: Do not use signal true: Use signal
EPON port link indication polarity: low	Polarity of the PON port link indication clock

Field		Description
CNI port link indication polarity:	high	Polarity of the CNI (System) port link indication clock
EPON tbc polarity:	low	Polarity of output TBC clock for the TBI bus
Discovery laser on time:	32	Laser on time adjustment to the ONUs during the discovery process, if any
Discovery laser off time:	32	Laser off time adjustment to the ONUs during the discovery process, if any
EPON Tx signal:	disable	The OLT PON Tx signal (disable or enable) When the signal is disabled, no data is transmitted on the PON

encryption timer

Syntax

encryption timer { **update-time** *update-time* | **no-reply-timeout** *timeout* }* **slot** *slot-number*

undo encryption timer slot *slot-number*

View

FTTH view

Default Level

2: System level

Parameters

update-time: Key update time, in seconds. It is in the range 1 to 255 and defaults to 10.

timeout: Encryption reply timeout time, in a unit of 100 ms. It is in the range 1 to 2550 and defaults to 30.

slot-number: Slot number of the EPON card.

Description

Use the **encryption timer** command to configure the key update time and encryption reply timeout time of the encryption.

Use the **undo encryption timer** command to restore the key update time and encryption reply timeout time of the encryption to the defaults.

Related command: **display epon-parameter**..

Caution

The encryption reply timeout time must be less than or equal to 10 times the key update time.

Examples

Configure the key update time and encryption reply timeout time for the EPON card in slot 3 as 20 seconds and 5 seconds (50 × 100 ms) respectively.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] encryption timer update-time 20 no-reply-timeout 50 slot 3
```

epon-parameter ouilist

Syntax

epon-parameter ouilist { **oui** *oui-value* **oam-version** *version-value* } *&<1-9>* **slot** *slot-number*

undo epon-parameter ouilist slot *slot-number*

View

FTTH view

Default Level

2: System level

Parameters

oui-value: OUI (Organizationally Unique Identifier) of the ONU.

version-value: OAM (Operation, Administration and Maintenance) version number of the ONU.

&<1-9>: Indicates that you can specify up to 9 OUI values/OAM version numbers.

slot-number: Slot number of the EPON card.

Description

Use the **epon-parameter ouilist** command to configure the OUI and extended OAM version number of the ONU in the specified slot.

Use the **undo epon-parameter ouilist** command to cancel the configuration.

By default, the OUI and extended OAM version number are 111111 and 1 respectively. After this configuration, an H3C ONU attached to an OLT goes online after being bound with the specified ONU port (The OUI and extended OAM version number for an H3C ONU are 111111 and 1 respectively).

Note the following:

- Entries with the same OUIs and extended OAM version numbers cannot be not configured at the same time on one EPON card.
- When the OUI and extended OAM version number list of an EPON card changes (when a list is configured or canceled), all the ONUs under the EPON card will reregister.

Related commands: **display epon-parameter**.

Examples

Configure the OUI and extended OAM version number of the ONU connected to the EPON card in slot 3.

```
<Sysname> system-view
[Sysname] ftth
```

```
[Sysname-ftth] epon-parameter ouilist oui 111111 oam-version 2 slot 3
```

fiber-backup group

Syntax

fiber-backup group *group-number*

undo fiber-backup group *group-number*

View

FTTH view

Default Level

2: System level

Parameters

group-number: Fiber backup group number, in the range 1 to 80.

Description

Use the **fiber-backup group** command to create a fiber backup group and enter fiber backup group view or directly enter fiber backup group view if the fiber backup group already exists.

Use the **undo fiber-backup group** command to delete a fiber backup group.

Caution

You can only delete a fiber backup group without any member ports.

Examples

Create fiber backup group 1 and enter fiber backup group view.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
 Create group 1 successfully.
[Sysname-fiber-group1]
```

grant-filtering enable

Syntax

grant-filtering enable

undo grant-filtering enable

View

OLT port view

Default Level

2: System level

Parameters

None

Description

Use the **grant-filtering enable** command to enable the grant filtering function on the OLT port.

Use the **undo grant-filtering enable** command to disable the grant filtering function on the OLT port.

By default, this function is enabled.

Examples

Enable grant filtering on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] grant-filtering enable
```

group member

Syntax

group member *interface-type interface-number*

undo group member *interface-type interface-number*

View

Fiber backup group view

Default Level

2: System level

Parameters

interface-type: Port type. It is OLT

interface-number: OLT port number.

Description

Use the **group member** command to add an OLT port to a fiber backup group (the group must exist).

Use the **undo group member** command to remove an OLT port from a fiber backup group.

Related commands: **fiber-backup group**.

Examples

In fiber backup group view, add OLT 3/0/1 to fiber backup group 1.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
Create group ID successfully.
[Sysname-fiber-group1] group member olt3/0/1
```

max-rtt

Syntax

max-rtt *value*

undo max-rtt

View

OLT port view

Default Level

3: Manage level

Parameters

max-rtt *value:* Maximum round trip time (RTT) to be set. This argument ranges from 1000 to 25000 (in TQs). The system default is 13524 TQs.

Description

Use the **max-rtt** command to set the maximum RTT from the ONU to the OLT.

 **Caution**

- Configure the maximum RTT from the ONU to the OLT only when necessary. The relationship between the RTT and the distance (in meters) from the OLT to the ONU can be expressed by the formula: RTT = (Distance + 157)/1.6393.
- The **max-rtt** command is applicable to unregistered ONUs only.
- For details about RTT, refer the related sections in the operation manual.

Examples

Set the maximum RTT of the ONU connected to OLT 3/0/1 to 25000 TQ.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] max-rtt 25000
```

multicast vlan-id dest-ip

Syntax

multicast vlan-id *vlan-id* **dest-ip** *ip-address-list*

undo multicast vlan-id *vlan-id* **dest-ip** *ip-address-list*

View

FTTH view

Default Level

1: Monitor level

Parameters

vlan-id: Multicast VLAN ID, in the range 1 to 4094.

ip-address-list: Multicast IP address(es). *ip-address-list* = { *ip-address* **|** *ip-address* **to** *ip-address* } &<1-10>.

&<1-10>: Indicates that you can specify up to 10 IP addresses/IP address ranges.

Description

Use the **multicast vlan-id dest-ip** command to add multicast address(es) to a multicast VLAN. Upon receiving an IGMP Report message, the OLT determines whether the multicast IP address contained in the message belongs to the multicast VLAN. If yes, the OLT generates a multicast forwarding entry in the multicast VLAN of the multicast IP address; otherwise, the OLT directly discards the message.

Use the **undo multicast vlan-id dest-ip** command to remove the configuration.

Note that a multicast IP address can belong to only one multicast VLAN.

Examples

Add multicast IP address 225.1.2.1 to multicast VLAN 1002.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] multicast vlan-id 1002 dest-ip 225.1.2.1
```

port fiber-backup group

Syntax

port fiber-backup group *group-number*

undo port fiber-backup group

View

OLT port view

Default Level

2: System level

Parameters

group-number: Fiber backup group number, in the range 1 to 80.

Description

Use the **port fiber-backup group** command to add the OLT port to the specified fiber backup group (the group must exist).

Use the **undo group member** command to remove the OLT port from the fiber backup group.

Related commands: **fiber-backup group**.

Examples

In OLT port view, add OLT 3/0/1 to fiber backup group 1.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
Create group ID successfully.
[Sysname-fiber-group1] quit
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port fiber-backup group 1
```

port hybrid pvid vlan

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

View

OLT port 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.

Note

To add default VLAN tags to the untagged inbound packets on an OLT port, make sure the default VLAN ID is configured for the OLT port and QinQ is enabled on the port (by using the **qinq enable** command).

Examples

Configure VLAN 100 as the default VLAN of the hybrid port OLT 2/0/1.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface olt 2/0/1
[Sysname-Olt2/0/1] 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

OLT port 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 hybrid port to send the packets of the specified VLAN(s) with the tags kept.

untagged: Configures the hybrid 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 to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current hybrid port 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.

Related commands: **port link-type**, **port hybrid pvid vlan**.

Examples

Assign the hybrid port OLT 3/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100, and configure OLT 3/0/1 to send packets of these VLANs with tags kept.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port link-type hybrid
[Sysname-Olt3/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

port link-type hybrid

Syntax

port link-type hybrid

View

OLT port view

Default Level

2: System level

Parameters

None

Description

Use the **port link-type hybrid** command to configure the OLT port as a hybrid port.

By default, any OLT port is an hybrid port.

Related commands: **port hybrid vlan**, **port hybrid pvid vlan**.

Examples

Configure OLT 3/0/1 as a hybrid port.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port link-type hybrid
```

port switch-over

Syntax

port switch-over

View

Fiber backup group view

Default Level

2: System level

Parameters

None

Description

Use the **port switch-over** command to perform a master/slave switchover between the two OLT ports in the fiber backup group.

After this command is executed, the original master OLT port becomes the new slave, while the original slave OLT port becomes the new master.

Note that the slave OLT must be in the ready state for a switchover to happen.

Related commands: **display fiber-backup group**.

Examples

Perform a manual master/slave switchover between the two OLT ports in fiber backup group 1.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
[Sysname-fiber-group1] port switch-over
```

using onu

Syntax

using onu { *onu-number1* [**to** *onu-number2*] } *&<1-10>*

undo using onu { *onu-number1* [**to** *onu-number2*] } *&<1-10>*

View

OLT port view

Default Level

2: System level

Parameters

onu-number1: ONU port number, in the range 1 to 64.

to *onu-number2*: Specifies an ONU port range. *onu-number2* is an ONU port number, in the range 1 to 64.

&<1-10>: Indicates that you can specify up to 10 ONU port numbers/port ranges.

Description

Use the **using onu** command to create virtual ONU port(s) for the current OLT port.

Use the **undo using onu** command to remove the specified ONU port(s) under the current OLT port.

By default, no ONU port is created for any OLT port when the EPON card is started up.

To use the **interface** command to enter ONU port view, use the **using onu** command to create the corresponding ONU port first.

Examples

Create ONU 3/0/1:5 whose sub-channel number is 5 for OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 5
Please wait…Done.
```

Create ONU ports whose sub-channel numbers are 1 to 5 for OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 1 to 5
Please wait….Done.
[Sysname-Olt3/0/1] display brief interface onu
The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
Onu3/0/1:1           DOWN      --           --       access     1
Onu3/0/1:2           DOWN      --           --       access     1
Onu3/0/1:3           DOWN      --           --       access     1
Onu3/0/1:4           DOWN      --           --       access     1
Onu3/0/1:5           DOWN      --           --       access     1
```

2 ONU Remote Management Configuration Commands

ONU Remote Management Configuration Commands

bind onuid

Syntax

bind onuid *onuid*

undo bind onuid

View

ONU port view

Default Level

2: System level

Parameters

onuid: MAC address of the ONU to be bound, in the *H-H-H* format.

Description

Use the **bind onuid** command to bind the current ONU port to an ONU by associating the ONU port with the MAC address of the ONU.

Use the **undo bind onuid** command to unbind the ONU port from the ONU. The unbinding operation invalidates all related configuration for the ONU.

Caution

- An ONU port can be bound with only one ONU MAC address. Conversely, an ONU MAC address can be bound with only one ONU port under one OLT port.
- In fiber backup, an ONU can be bound with two ONU ports under two OLT ports acting as backups for each other.

Examples

Bind port ONU 3/0/2:1 to an ONU whose MAC address is 000f-e200-0104.

```
<Sysname> system-view
[Sysname] interface onu 3/0/2:1
[Sysname-Onu3/0/2:1] bind onuid 000f-e200-0104
```

dba-report queue-id threshold

Syntax

dba-report queue-id *queue-id* { **active | inactive** } **threshold** *threshold-value*

undo dba-report queue-id

View

ONU port view

Default Level

2: System level

Parameters

queue-id: Queue number in the range 1 to 8.

threshold-value: Threshold of a queue, in the range 0 to 65535. The default thresholds of queue 4 and queue 5 are 65535, and the default thresholds of other queues are 0.

active: Activates the threshold.

inactive: Inactivates the threshold.

Description

Use the **dba-report queue-id threshold** command to configure the threshold for a queue.

Use the **undo dba-report queue-id** command to restore the default threshold for a queue.

Examples

Configure the threshold of queue 1 as 200 and activate the threshold.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] dba-report queue-id 1 active threshold 200
```

dba-report queue-set-number

Syntax

dba-report queue-set-number *queue-set-number*

undo dba-report queue-set-number

View

ONU port view

Default Level

2: System level

Parameters

queue-set-number: Number of queue sets. It is in the range 2 to 4 and defaults to 2.

Description

Use the **dba-report queue-set-number** command to configure the number of queue sets supported by ONU Report frames.

Use the **undo dba-report queue-set-number** command to restore the default number of queue sets supported by ONU Report frames.

 **Caution**

H3C's ONU Report frames support up to two queue sets.

Examples

Configure the number of queue sets supported by ONU Report frames as 2.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] dba-report queue-set-number 2
```

deregister onu

Syntax

deregister onu

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **deregister onu** command to deregister the ONU under the ONU port.

Examples

Deregister the ONU under ONU port ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] deregister onu
```

display dhcp-client

Syntax

display dhcp-client

View

ONU port view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp-client** command to display the IP address allocation information when the ONU serves as a DHCP client.

Examples

Display the IP address allocation information when the ONU serves as a DHCP client.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] display dhcp-client
DHCP client statistic information:

  Current machine state : BOUND
  Allocated IP          : 192.168.0.7        255.255.255.0
  Gateway IP            : 192.168.0.2
  Server IP             : 192.168.0.1
  Allocated lease       : 86400  seconds
  T1 to renew           : 43200  seconds
  T2 to rebind          : 75600  seconds
  T1 left               : 43197  seconds
  T2 left               : 75597  seconds
```

This displays shows that the allocated IP address is 192.168.0.7, with subnet mask 255.255.255.0, and that the gateway IP address is 192.168.0.2.

Table 2-1 display dhcp-client command output description

Field	Description
Current machine state	State of the DHCP client state machine
Allocated IP	IP address allocated to the DHCP client
Server IP	Selected DHCP server address
Allocated lease	Lease period
T1 to renew	The 1/2 lease time (in seconds) of the DHCP client IP address
T2 to rebind	The 7/8 lease time (in seconds) of the DHCP client IP address
Server IP	Selected DHCP server address

display epon-multicast information

Syntax

display epon-multicast information

View

ONU port view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display epon-multicast information** command to display multicast control information.

Examples

Display multicast control information when the multicast mode of the ONU is IGMP snooping.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] display epon-multicast information
 ONU is not in multicast-control mode.
```

Display multicast control information when the multicast mode of the ONU is multicast control mode but no multicast control information is generated.

```
[Sysname-Onu3/0/1:1] display epon-multicast information
 Multicast-control information: None.
```

Display multicast control information when the multicast mode of the ONU is multicast control mode and multicast control information is generated.

```
[Sysname-Onu3/0/1:1] display epon-multicast information
 Multicast-control information:
------------------------------
 UNI number 1:
 Multicast vlan 10
 Current channel list:
 multicast ip:225.0.0.2
 status:permit

 Multicast vlan 10
 Current channel list:
 multicast ip:225.0.0.3
 status:preview
 preview times:16
 preview remain time:144s
```

Table 2-2 display epon-multicast information command output description

Field	Description
ONU is not in multicast-control mode.	The multicast control mode of the ONU is IGMP snooping. No multicast control information is available now.
Multicast-control information: None.	The multicast control mode of the ONU is multicast control mode but no multicast control information is generated. There are two reasons for this: • No multicast control contents are configured. • The multicast client sends no IGMP report message.
UNI number 1	UNI port number
Multicast vlan 10	Multicasts VLAN number
Current channel list	List of current multicast channels
multicast ip	Multicast IP address of multicast channel
status:permit	Multicast control policy permit: Allows access to the corresponding multicast channel (without time limit). preview: Allows previewing the corresponding multicast channel (with time limit)
preview times:16	This is the sixteenth time the corresponding multicast channel has been previewed.
preview remain time:144s	The channel can be previewed for 144 more seconds before the preview ends.

display onu-protocol

Syntax

display onu-protocol [**stp** | **igmp-snooping | dhcp-snooping information**]

View

ONU port view

Default Level

2: System level

Parameters

stp: Displays the information about RSTP supported by the ONU.

igmp-snooping: Displays the information about IGMP snooping supported by the ONU.

dhcp-snooping information: Displays the information about DHCP-Snooping Option82 supported by the ONU.

Description

Use the **display onu-protocol** command to display the information about the protocols supported by an ONU that is in up state.

If no parameter is specified, the information about all the protocols that the ONU supports is displayed.

Caution

- This command takes effect on H3C ONUs only.
- STP runs normally only when all attached ONUs are H3C ONUs.

Examples

Display the information about IGMP snooping supported by the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] display onu-protocol igmp-snooping
  Protocol name: IGMP snooping
  Protocol status: enabled
  Multicast Address    UNI Port   VLAN
1 01:00:5e:01:01:01    2            10
2 01:00:5e:01:01:02    3            20
```

Table 2-3 display onu-protocol igmp-snooping command output description

Field	Description
Protocol name: IGMP snooping	Protocol name
Protocol status: enabled	Protocol status: enabled or disabled
Multicast Address	Multicast MAC address
UNI Port	UNI port number
VLAN	Multicast VLAN number

display vendor-specific information

Syntax

display vendor-specific information

View

ONU port view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display vendor-specific information** command to display the detailed information of the ONU when it is up.

Examples

Display the detailed ONU information of ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] display vendor-specific information
serial number
     vendor id : H3C
     onu mac address : 000f-e276-4b93
     onu model : 0x704
     onu hardware version : B
     onu software version : 110
 firmware version : 0x214
 chipset information :
     vendor id : 0x4536
     chip model : 6301
     revision version : 0x00
     design date : 07/09/27
 onu capability :
     gigabit ethernet interface :  not support
     fast ethernet interface :  support
     voip service :  not support
     tdm ces service :  not support
     gigabit ethernet ports number :  0
     fast ethernet ports number :  4
     fast ethernet ports :
       0x1
       0x2
       0x3
       0x4
     pots ports number :  0
     e1 ports number :  0
     upstream queues number :  4
     Maximum queues per port upstream :  4
     downstream queues number :  4
     Maximum queues per port downstream :  4
     battery backup :  not support
 forward error correction ability : support
 forward error correction mode : disable
 DBA-Report parameters :
      queue sets number : 2
      queue 1 : state:1 , value:0
      queue 2 : state:1 , value:0
      queue 3 : state:1 , value:0
```

```
     queue 4 : state:1 , value:65535
     queue 5 : state:1 , value:65535
     queue 6 : state:1 , value:0
     queue 7 : state:1 , value:0
     queue 8 : state:1 , value:0
Multicast-mode : multicast control
```

Table 2-4 display vendor-specific information command output description

Field	Description
gigabit ethernet interface : not support	Whether the ONU has Gigabit Ethernet ports
fast ethernet interface : support	Whether the ONU has fast Ethernet ports
voip service : not support	Whether the ONU supports Voice over IP (VoIP) service
tdm ces service : not support	Whether the ONU supports the TDM Circuit Emulation Service (CES)
gigabit ethernet ports number : 0	Number of Gigabit Ethernet ports
fast ethernet ports number : 4	Number of fast Ethernet ports
fast ethernet ports : 0x1 0x2 0x3 0x4	Fast Ethernet port numbers: 1, 2, 3, 4
pots ports number : 0	Number of Plain Old Telephone Service (POTS) ports
e1 ports number : 0	Number of E1 ports
upstream queues number : 4	Number of upstream queues
Maximum queues per port upstream : 4	Maximum number of upstream queues supported per port
downstream queues number : 4	Number of downstream queues
Maximum queues per port downstream : 4	Maximum number of downstream queues supported per port
battery backup : not support	Whether battery backup is supported
forward error correction ability : support	Whether Forward Error Correction (FEC) is supported
forward error correction mode : disable	Whether FEC is enabled
queue sets number : 2	Number of queue sets supported
queue 1 : state:1 , value:0 queue 2 : state:1 , value:0 queue 3 : state:1 , value:0 queue 4 : state:1 , value:65535 queue 5 : state:1 , value:65535 queue 6 : state:1 , value:0 queue 7 : state:1 , value:0 queue 8 : state:1 , value:0	Queue states and thresholds. If the value of **state** is 0, it means the queue is disabled; if the value of **state** is 1, it means the queue is enabled.

Field	Description
Multicast-mode : multicast control	Multicast mode: IGMP Snooping (IGSP) or multicast control

display uni-information

Syntax

display uni-information *uni-number*

View

ONU port view

Default Level

1: Monitor level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **display uni-information** command to display the state information about the current UNI.

Caution

This command takes effect on H3C ONUs only.

Examples

Display the state information about UNI 1 of the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] display uni-information 1
uni-number : 1
 flow-control : closed
 PHY admin state for ethernet port : UP
 port-policy :
   inbound :
     CIR : 102400
     Bucket depth : 0
     Extra burst size : 0
   outbound :
     CIR : 102400
 Vlan-configration :
     Current-vlan-mode : transparent
```

```
Multicast-vlan :
Multicast-group-number : 64
Auto-negotiation state : enable
Multicast-strip-tag : disable
Link-state : UP
Auto-negotiation local technology ability :
    100BASE-TX
    Full duplex 100BASE-TX
    Full duplex 10BASE-T
    10BASE-T
    Symmetric PAUSE operation for full duplex links
    Asymmetric PAUSE operation for full duplex links
Auto-negotiation advertised technology ability :
    Full duplex 100BASE-TX
100Mbps-speed mode, Full-duplex mode
Link speed type is autonegotiation, Link duplex type is autonegotiation
Port-isolate is not enabled
Mdi type: auto
Input(total):  202 packets, 15270 bytes
         8 broadcasts, 0 multicasts, 194 unicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 InRxErr, 0 CRC
        0 buffer failures
Output(total): 44644 packets, 2959256 bytes
         37035 broadcasts, 7312 multicasts, 297 unicasts, 0 pauses
Output: 0 output errors, 0 deferred, 0 collisions, 0 InTxErr
```

Table 2-5 display uni-information command output description

Field	Description
uni-number : 1	UNI port number
flow-control : closed	Whether flow control is enabled
PHY admin state for ethernet port : UP	Administrative state of the port, which can be: • UP: The port is brought up with the **undo shutdown** command. • DOWN: The port is manually shut down.
port-policy : inbound : CIR : 102400 Bucket depth : 0 Extra burst size : 0 outbound : CIR : 102400	Upstream/downstream traffic policing parameters of the UNI: • inbound: Upstream traffic policing parameters • outbound: Downstream traffic policing parameters
Vlan-configration : Current-vlan-mode : transparent	VLAN mode
Multicast-vlan : Multicast-group-number : 64	Number of multicast groups supported by the UNI

Field	Description
Auto-negotiation state : enable	Whether auto-negotiation is enabled
Multicast-strip-tag : disable	Whether it is enabled to strip the VLAN tag off the downstream multicasts on the UNI
Link-state : UP	Layer-2 link state
Auto-negotiation advertised technology ability : Full duplex 100BASE-TX	Auto-negotiation advertisement ability
Port-isolate is not enabled	Whether the UNI is added to a port isolation group
Input(total): 202 packets, 15270 bytes 8 broadcasts, 0 multicasts, 194 unicasts, 0 pauses	Totally, 202 packets (15270 bytes) are received. Among these packets, there are eight broadcast packets, 0 multicast packets, 194 unicast packets, and 0 pause frames.
Input: 0 input errors, 0 runts, 0 giants, 0 InRxErr, 0 CRC 0 buffer failures	0 error frames, 0 runts, and 0 giants are received. There are 0 buffer failures.
Output(total): 44644 packets, 2959256 bytes 37035 broadcasts, 7312 multicasts, 297 unicasts, 0 pauses	Totally, 44644 packets (2959256 bytes) are sent, including 37035 broadcast packets, 7312 multicast packets, 297 unicast packets, and 0 pause frames.
Output: 0 output errors, 0 deferred, 0 collisions, 0 InTxErr	There are 0 output errors, 0 deferred packets, 0 collisions, and 0 error packets in transmission.

Note

- A runt is a frame that has a length less than 64 bytes in a correct format and contains a valid CRC field.
- A giant is a frame that has a valid length greater than 1518 bytes (without VLAN tag) or 1522 bytes (with VLAN tag).
- Buffer failures indicate the number of packets discarded due to insufficient transmit buffer on the port.
- A deferred packet means a packet whose transmission is delayed upon detection of a collision before the transmission.
- A collision frame refers to a packet whose transmission is stopped upon detection of a collision during the packet transmission.

encrypt enable

Syntax

encrypt enable

undo encrypt enable

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **encrypt enable** command to encrypt downstream data.

Use the **undo encrypt enable** command to disable stream encryption.

By default, encryption is enabled for downstream data.

Examples

Enable downstream data encryption.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] encrypt enable
```

encrypt key

Syntax

encrypt key *key-value*

undo encrypt key

View

ONU port view

Default Level

2: System level

Parameters

key-value: Encryption key, a string of up to 16 characters.

Description

Use the **encrypt key** command to configure the encryption key.

Use the **undo encrypt** command to restore the default encryption key.

Caution

- This command takes effect on H3C ONUs only.
- Currently, the **encrypt key** command is not supported.

Examples

Configure the encryption key as **test**.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] encrypt key test
 This operation is not supported in current version!
```

forward-error-correction enable

Syntax

forward-error-correction enable

undo forward-error-correction enable

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **forward-error-correction enable** command to enable forward error correction (FEC) on the OLT and ONUs.

Use the **undo forward-error-correction enable** command to disable this function.

This function is disabled by default.

Examples

Enable FEC on the OLT and ONUs.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] forward-error-correction enable
```

ip address

Syntax

ip address { **dhcp-alloc** | *ip-address mask* **gateway** *gateway* }

undo ip address

View

ONU port view

Default Level

2: System level

Parameters

dhcp-alloc: Obtains an IP address through DHCP.

ip-address: IPv4 address.

mask: Subnet mask, in dotted decimal notation or integer in the range 0 to 32 (indicating the network address length).

gateway: Specifies a gateway IP address.

Description

Use the **ip address** command to manually configure an IP address or obtain one through DHCP for the ONU.

Use the **undo ip address** command to restore the default.

By default, no IP address is configured for the ONU, either manually or automatically through DHCP.

Examples

Configure the IP address of the ONU as 192.168.0.1/24 and gateway as 192.168.0.99.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] ip address 192.168.0.1 24 gateway 192.168.0.99
```

linktest

Syntax

linktest [**frame-number** *value* | **frame-size** *value* | **delay** { **on** | **off** } | **vlan-tag**

{ **on** [**vlan-priority** *value* | **vlan-id** *value*] | **off** }] *

View

ONU port view

Default Level

2: System level

Parameters

frame-number *value*: Specifies the number of test frames. The *value* argument ranges from 1 to 250 and defaults to 20.

frame-size *value*: Specifies the test frame size in bytes. The *value* argument ranges from 60 to 1514 and defaults to 1000.

delay: Specifies whether or not to enable delay test. The **on** keyword enables delay test. The **off** keyword disables delay test.

vlan-tag: Specifies whether or not to insert VLAN tags in test frames. The **on** keyword specifies to insert VLAN tags in test frames. The **off** keyword specifies not to insert VLAN tags to test frames. By default, test frames contain VLAN tags.

vlan-priority *value*: Specifies the VLAN priority of test frames. The *value* argument ranges from 0 to 7, with value 0 representing the lowest priority, and value 7 representing the highest priority.

vlan-id *value*: Specifies the VLAN ID of test frames. The *value* argument ranges from 1 to 4094 and defaults to 1.

Description

Use the **linktest** command to test the connectivity of the optical link between the OLT and the ONU.

Make sure the ONU is online before you perform the link connectivity test.

Examples

Set the number of test frames to 100 to test the link between the OLT and ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] linktest frame-number 100
 It may affect data transmission, continue?[Y/N]:y
 Maximum delay(in TQ): 26408
 Mean delay(in TQ)   : 24777
 Minimum delay(in TQ): 19922
 Sent frames         : 100
 Received frames     : 100
 Error frames        : 0
```

Note

If **The link is disconnected!** is displayed, it means that the ONU sent some frames successfully but no correct frames are received, namely, the value of the **Received frames** field is 0.

loopback enable

Syntax

loopback enable

undo loopback enable

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **loopback enable** command to enable MAC loopback for the ONU.

Use the **undo loopback enable** command to cancel loopback.

By default, MAC loopback is not enabled for an ONU.

Related commands: **loopback** command in *Port Basic Configuration Commands.*

Note

- Use this command only when necessary as enabling MAC loopback for an ONU may affect the device performance.
- You need to use the **undo loopback enable** command to cancel the loopback, which does not end automatically.

Examples

Enable MAC loopback on ONU 3/0/1:1, and cancel the loopback one minute later.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1]loopback enable
 Warning: enable loopback will affect system performance and business, are you sure?(Y/N)y
[Sysname-Onu3/0/1:1]undo loopback enable
```

management-vlan

Syntax

management-vlan *vlan-id*

undo management-vlan

View

ONU port view

Default Level

2: System level

Parameters

vlan-id: Specifies the management VLAN ID, in the range 1 to 4094.

Description

Use the **management-vlan** command to configure the management VLAN of the ONU.

Use the **undo management-vlan** command to restore the default management VLAN ID of the ONU.

By default, VLAN 1 operates as the management VLAN of the ONU.

Examples

Configure the management VLAN of the ONU as VLAN 10.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] management-vlan vlan 10
```

multicast-control host-aging-time

Syntax

multicast-control host-aging-time *host-aging-time*

undo multicast-control host-aging-time

View

ONU port view

Default Level

1: Monitor level

Parameters

host-aging-time: Aging time of multicast group member port in multicast control mode, in seconds. It is in the range 200 to 1000 and defaults to 260.

Description

Use the **multicast-control host-aging-time** command to configure the aging time of multicast group member port in multicast control mode.

Use the **undo multicast-control host-aging-time** command to restore the default aging time of multicast group member port in multicast control mode.

By default, the aging time of a multicast group member port is 260 seconds.

Note that this command is available in multicast control mode only.

Examples

Configure the aging time multicast group member port in multicast control mode as 500 seconds.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] multicast-control host-aging-time 500
```

multicast-mode

Syntax

multicast-mode { **igmp-snooping** | **multicast-control** }

undo multicast-mode

View

ONU port view

Default Level

2: System level

Parameters

igmp-snooping: Specifies the IGMP Snooping mode.

multicast-control: Specifies the multicast control mode.

Description

Use the **multicast-mode** command to configure the multicast mode of the ONU.

Use the **undo multicast-mode** command to restore the default.

By default, the multicast mode of the ONU is IGMP Snooping.

Examples

Configure the multicast mode of the ONU as the multicast control mode.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] multicast-mode multicast-control
```

onu-event

Syntax

onu-event { **debug** | **log** | **trap** } **enable level** *severity*

undo onu-event { **debug** | **log** | **trap** }

View

ONU port view

Parameters

debug: Displays the types of debugging information allowed to be output by the ONU on the OLT.

log: Displays the log information generated by the ONU on the OLT.

trap: Displays the trap information generated by the OLT on the ONU.

severity: Severity level of the information that the ONU reports to the OLT. The severity levels include (in the descending order of priority):

emergencies, alerts, critical, errors, warnings, notifications, information, and debugging.

Description

Use the **onu-event** { **debug** | **log** | **trap** } **enable level** command to specify the ONU to report log, debugging, or trap information to the OLT.

Use the **undo onu-event** { **debug** | **log** | **trap** } command to restore the default.

By default, an ONU reports no information to the OLT.

Note that: because a large number of ONUs are attached to an OLT, enabling ONUs to report information to the OLT may generate a large amount of traffic and thus cause congestion. Therefore, you are recommended to select the reported information types as required.

Examples

Configure the OLT attached to ONU 3/0/1:1 to report log information with severity levels higher than **errors**.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu-event log enable level ?
  alerts         <=ALERT level messages to OLT    (severity=1)
```

```
  critical       <=CRIT level messages to OLT      (severity=2)
  debugging      <=DEBUG level messages to OLT     (severity=7)
  emergencies    <=EMERG Level Switch to OLT       (severity=0)
  errors         <=ERR level messages to OLT       (severity=3)
  information    <=INFO level messages to OLT      (severity=6)
  notifications  <=NOTICE level messages to OLT    (severity=5)
  warnings       <=WARN level messages to OLT      (severity=4)
[Sysname-Onu3/0/1:1] onu-event log enable level errors
```

Disable the OLT attached to ONU 3/0/3:1 from reporting log information to the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/3:1
[Sysname-Onu3/0/3:1] undo onu-event log enable
```

Table 2-6 onu-event log enable level command output description

Field	Severity level	Remarks
emergencies	0	Indicating that the system is unavailable.
alerts	1	Errors that need to be corrected immediately.
critical	2	Critical Information.
errors	3	Errors.
warnings	4	Warning Information.
notifications	5	Normal information that needs to be noticed.
information	6	Normal prompt information that needs to be recorded.
debugging	7	Debugging information.

onu port-isolate enable

Syntax

onu port-isolate enable

undo onu port-isolate enable

View

ONU port view

Parameters

None

Description

Use the **onu port-isolate enable** command to isolate all UNI ports of the ONU.

Use the **undo onu port-isolate enable** command to disable UNI port isolation.

By default, UNI port isolation is disabled.

Examples

Isolate all UNI ports attached to the ONU corresponding to ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu port-isolate enable
```

onu-protocol enable

Syntax

onu-protocol { **stp** | **dhcp-snooping** | **dhcp-snooping information** | **pppoe** } **enable**

undo onu-protocol { **stp** | **dhcp-snooping** | **dhcp-snooping information** | **pppoe** } **enable**

View

ONU port view

Default Level

2: System level

Parameters

stp: Enables RSTP for the ONU.

dhcp-snooping: Enables DHCP-Snooping for the ONU.

dhcp-snooping information: Enables DHCP-Snooping Option82 for the ONU.

pppoe: Enables PPPoE+ for the ONU.

Description

Use the **onu-protocol enable** command to enable RSTP, DHCP-Snooping, DHCP-Snooping Option82, or PPPoE+ for the ONU.

Use the **undo onu-protocol enable** command to disable the specified feature(s).

By default, RSTP is enabled for the ONU, while DHCP-Snooping, DHCP-Snooping Option82, and PPPoE+ are disabled for the ONU.

Caution

- This command takes effect on H3C ONUs only.
- STP runs normally only when all attached ONUs are H3C ONUs.
- When STP is enabled globally on the S7900E switch, make sure all the ONUs are enabled with STP and no ONU acts as an STP root bridge to avoid network anomalies.

Examples

Enable DHCP snooping on the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu-protocol dhcp-snooping enable
```

onu-protocol igmp-snooping

Syntax

onu-protocol igmp-snooping { **host-aging-time** *host-aging-time* | **leave-aggregation enable** | **max-response-time** *max-response-time* | **report-aggregation enable** | **router-aging-time** *router-aging-time* }

undo onu-protocol igmp-snooping { **host-aging-time** | **leave-aggregation enable** | **max-response-time** | **report-aggregation enable** | **router-aging-time** }

View

ONU port view

Default Level

2: System level

Parameters

host-aging-time: Aging time of multicast group member port, in seconds. It is in the range 200 to 1000 and defaults to 260.

leave-aggregation enable: Enables IGMP leave message suppression.

max-response-time: Maximum response time (in seconds) of group-specific queries. It is in the range 1 to 25 and defaults to 1.

report-aggregation enable: Enables IGMP report message suppression

router-aging-time: Router port aging time, in seconds. It is in the range 1 to 1000 and defaults to 105.

Note

The **max-response-time** keyword in the **onu-protocol igmp-snooping** command sets the maximum response time of the group-specific queries. If the device receives no response at the first timeout of the maximum response time, it re-sends group-specific queries. If the device still receives no response within the maximum response time, the multicast group on the corresponding ONU is deleted.

Description

Use the **onu-protocol igmp-snooping** command to configure IGMP snooping-related timers and IGMP membership report suppression.

Use the **undo onu-protocol igmp-snooping** command to restore the defaults.

By default, IGMP join suppression is disabled, while IGMP leave suppression is enabled.

Note the following:

- The aging time of multicast group member ports determines how often multicast group members are refreshed. In an environment where multicast group members change frequently, a relatively shorter aging time is required.

- The router port here refers to the port connecting the ONU to the router. The ONU receives IGMP general query messages from the router through this port. The aging time of the router port should be a value about 2.5 times of the general query interval.
- This command takes effect on H3C ONUs only.

Examples

Enable IGMP join suppression on the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu-protocol igmp-snooping report-aggregation enable
```

port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

View

ONU port view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4,094

Description

Use the **port access vlan** command to add the current Access port to the specified VLAN.

Use the **undo port access vlan** command to add the current Access port to the default VLAN.

By default, all Access ports are added to VLAN 1.

Ensure the VLAN specified by the *vlan-id* argument exists before issuing the above commands.

Examples

Add port ONU3/0/1:1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] port access vlan 3
```

port link-type

Syntax

port link-type { **access** | **trunk** }

undo port link-type

View

ONU port view

Default Level

2: System level

Parameters

access: Configures the link type of an ONU port as Access.

trunk: Configures the link type of an ONU port as Trunk.

Description

Use the **port link-type** command to configure the link type of an ONU port.

Use the **undo port link-type** command to restore the default link type of an ONU port, which is Access by default.

Note

After an ONU port is configured as a trunk port, the ONU port allows the packets of all the VLANs to pass through.

Examples

Configure port ONU 3/0/1:1 to be a Trunk port.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] port link-type trunk
```

port trunk pvid vlan

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

View

ONU port view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4,094

Description

Use the **port trunk pvid vlan** command to set the default VLAN ID of the ONU port configured as a trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN on a Trunk port is VLAN 1.

For a Trunk port, after you execute the **undo vlan** command to remove the default VLAN of the Trunk port, the default VLAN of the Trunk port does not change. That is to say, the Trunk port can use the non-existing VLAN as the default VLAN.

Related commands: **port link-type**.

Examples

Configure the default VLAN ID for the Trunk port ONU 3/0/1:1 as 100.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] port link-type trunk
[Sysname-Onu3/0/1:1] port trunk pvid vlan 100
```

reboot onu

Syntax

reboot onu

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **reboot onu** command to restart the ONU.

Before using this command, make sure the ONU is online.

Examples

Restart ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] reboot onu
```

reset counters uni

Syntax

reset counters uni [*uni-number*]

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the maximum number of UNI ports supported by the ONU. By default, the maximum number is 80.

Description

Use the **reset counters uni** command to clear the counter information of the specified UNI port.

If no UNI is specified, the counter information of all the UNIs of the ONU is cleared.

Caution

- This command takes effect on H3C ONUs only.
- To use this command, make sure the ONU is up.

Related commands: **display uni-information**.

Examples

Clear the counter information of UNI port 1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] reset counters uni 1
```

shutdown management-vlan-interface

Syntax

shutdown management-vlan-interface

undo shutdown management-vlan-interface

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **shutdown management-vlan-interface** command to shut down the management VLAN interface of the ONU.

Use the **undo shutdown management-vlan-interface** command to bring up the management VLAN interface of the ONU.

By default, a management VLAN interface is down.

After the **undo shutdown management-vlan-interface** command is used:

- A management VLAN interface is down if all the Ethernet ports in the management VLAN of the ONU are down;
- A management VLAN interface is up if one or more Ethernet ports in the management VLAN of the ONU are up.

Examples

Bring up the management VLAN interface of the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] undo shutdown management-vlan-interface
```

uni auto-negotiation

Syntax

uni *uni-number* **auto-negotiation**

undo uni *uni-number* **auto-negotiation**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni auto-negotiation** command to enable auto-negotiation on a UNI port.

Use the **undo uni auto-negotiation** command to disable auto-negotiation on a UNI port.

By default, auto-negotiation is enabled on a UNI port.

Caution

When auto-negotiation is enabled on a UNI port, you cannot configure the duplex state, MDI mode, or rate of the UNI port.

Examples

Enable auto-negotiation on UNI port 1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 auto-negotiation
```

uni description

Syntax

uni *uni-number* **description** *text*

undo uni *uni-number* **description**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number of an ONU, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

text: String of 1 to 40 characters describing the UNI.

Description

Use the **uni description** command to configure a description for a UNI.

Use the **undo uni** *uni-number* **description** command to restore the default.

By default, no description is configured for a UNI.

Examples

Configure the description of UNI 1 as **Test**.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 description Test
```

uni duplex

Syntax

uni *uni-number* **duplex** { **full** | **half** | **auto** }

undo uni *uni-number* **duplex**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

full: Specifies the port to be in full duplex mode.

half: Specifies the port to be in half duplex mode.

auto: Specifies the duplex mode of the port to be auto-negotiation.

Description

Use the **uni duplex** command to set the duplex mode for UNIs.

Use the **undo uni duplex** command to restore the duplex mode on the current port to the default value.

By default, the duplex mode on UNIs is full.

 **Caution**

This command takes effect on H3C ONUs only.

Examples

Configure UNI 1 to operate in the auto-negotiation mode.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 duplex auto
```

uni flow-control

Syntax

uni *uni-number* **flow-control**

undo uni *uni-number* **flow-control**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni flow control** command to enable flow control for a UNI.

Use the **undo uni flow-control** command to disable flow control.

By default, flow control is disabled on a UNI.

Examples

Enable flow control for UNI 1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 flow-control
```

uni igmp-snooping fast-leave

Syntax

uni *uni-number* **igmp-snooping fast-leave**

undo uni *uni-number* **igmp-snooping fast-leave**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni igmp-snooping fast-leave** command to enable fast leave on the UNI.

Use the **undo uni igmp-snooping fast-leave** command to disable this function.

By default, fast leave is disabled on a UNI.

Examples

Enable fast leave on UNI 1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 igmp-snooping fast-leave
```

uni mdi

Syntax

uni *uni-number* **mdi** { **across** | **auto** | **normal** }

undo uni *uni-number* **mdi**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

across: Specifies the cable type to be crossover.

auto: Specifies to auto-sense the cable type.

normal: Specifies the cable type to be straight-through.

Description

Use the **uni mdi** command to set the MDI mode for UNIs.

Use the **undo uni** *uni-number* **mdi** command to restore the MDI mode for UNIs to the default value.

By default, the MDI mode for UNIs is **auto**, that is, the UNIs of the ONU can recognize the cable type automatically.

 **Caution**

This command takes effect on H3C ONUs only.

Examples

Set the MDI mode of UNI 1 to **auto**.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 mdi auto
```

uni multicast vlan

Syntax

uni *uni-number* **multicast vlan** { *vlan-id* } *& <1-50>*

undo *uni-number* **multicast vlan** { { *vlan-id* } *& <1-50>* | **all** }

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

vlan-id: Multicast VLAN ID, in the range 1 to 4094. *&<1-50>* means that you can provide up to 50 VLAN IDs for this argument.

all: Specifies all the multicast VLAN IDs.

Description

Use the **uni multicast vlan** command to add a UNI to the specified multicast VLAN(s).

Use the **undo uni multicast vlan** command to remove a UNI from the specified multicast VLAN(s).

This command takes effect only when the ONU works in the IGMP snooping mode.

Related commands: **multicast-mode**.

Examples

Add UNI 1 to multicast VLAN 200 and multicast VLAN 3000.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 multicast vlan 2000 3000
```

uni multicast-control multicast-address

Syntax

uni *uni-number* **multicast-control multicast-address** { *multicast-address* [**to** *multicast-address*] } &<1-10> [**source-ip** *ip-address* [**to** *ip-address*]] **rule** { **deny** | **permit** [**channel-limit** *channel-number*] | **preview time-slice** *preview-time* [**preview-interval** *interval-time* | **preview-times** *preview-times* [**reset-interval** *reset-interval-time*]]* }

undo uni *uni-number* **multicast-control multicast-address** [*multicast-address* [**to** *multicast-address*]] &<1-10>

View

ONU port view

Default Level

1: Monitor level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

multicast-address: Multicast IP address(es). *&<1-10>* means that you can specify up to 10 multicast IP addresses/multicast IP address ranges.

ip-address: IP address of the multicast source

deny: Denies access.

permit: Permits access.

channel-number: Number of channels that can be accessed at the same time, in the range 1 to 5.

preview-time: Allowed preview time, in minutes. It is in the range 1 to 3.

interval-time: Allowed preview interval., in minutes. It is in the range 1 to 10.

preview-times: Allowed preview times, in the range 1 to 3.

reset-interval-time: Preview reset interval, namely, time elapsed (in minutes) after the preset number of preview times is reached and before the next preview can be performed. It is in the range 1 to 43200.

Description

Use the **uni multicast-control multicast-address** command to configure the access (permit, preview, or deny) to multicast channels for the users connected to the specified UNI.

Use the **undo uni multicast-control multicast-address** command to remove the configuration.

Note that this command is available in multicast control mode only.

If this command is executed with the **source-ip** keyword, the OLT will process the received IGMPv3 packets as follows:

- For IS_IN, TO_IN, or ALLOW IGMPv3 packets, if the multicast IP address and source IP address carried in the packets are within the range configured for the multicast rights, the OLT creates the multicast table entries; otherwise, the OLT discards the packets.
- If the packet type is IS_EX or TO_EX, the OLT discards the packets.
- If the packet type is BLOCK, the OLT directly deletes the corresponding multicast table entries without checking the packet rights.

For details about IS_IN, TO_IN, ALLOW, IS_EX, TO_EX, and BLOCK IGMPv3 packets, see *IGMP Operation* in the *IP Multicast Volume*.

Examples

Allow all the users connected to UNI 1 to access the multicast channels with the multicast IP address 224.1.1.2.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 multicast-control multicast-address 224.1.1.2 rule permit
```

uni multicast-group-number

Syntax

uni *uni-number* **multicast-group-number** *number*

undo uni *uni-number* **multicast-group-number**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

number: Number of multicast channels, in the range 0 to 255.

Description

Use the **uni multicast-group-number** command to configure the number of multicast channels that can be accessed at the same time by the users connected to the specified UNI of the ONU.

Use the **undo uni multicast-group-number** command to restore the default value.

By default, the users connected to a UNI can access up to 64 multicast channels at the same time.

This command takes effect only when the ONU works in the IGMP snooping mode.

Related commands: **multicast-mode**.

The maximum number of multicast channels supported by the UNI ports of an H3C ONU varies with ONU type, as shown in the following table.

Table 2-7 Maximum number of multicast channels supported by H3C ONUs

H3C ONU type	Maximum number of multicast channels supported by UNI ports
S3100-SI series	256
S3100-EI series	512
ET704 series	64
ET254-L	Multicast not supported

Assume the maximum number of multicast channels supported by the UNI ports of an ONU is less than the maximum number of channels configured remotely through OLT:

- When the ONU is online, if you configure the maximum number of multicast channels on UNI ports to be greater than that supported by the UNI ports, the configuration will fail. For example, the UNI ports of an ET704 series ONU support up to 64 multicast channels. If you use the **uni multicast-group-number** command by specifying a value greater than 64 for the *number* argument through the OLT, a message prompt will be displayed indicating the configuration fails.
- When the ONU is not online, if you configure the maximum number of multicast channels on UNI ports through the OLT to be greater than that supported by the UNI ports, after the ONU goes online, the ONU will use the maximum number supported. For example, if you configure the maximum number of multicast channels on the UNI ports as 255 through the OLT while the maximum number of multicast channels supported on the UNI ports of an ET704 series ONU is 64, the ONU will support 64 multicast channels.

Examples

Allow the users connected to UNI 1 of the ONU to access up to 32 multicast channels at the same time.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 multicast-group-number 32
```

uni multicast-strip-tag enable

Syntax

uni *uni-number* **multicast-strip-tag enable**

undo uni *uni-number* **multicast-strip-tag enable**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni multicast-strip-tag enable** command to configure the specified UNI to remove the VLAN tag of the downlink multicast flow.

Use the **undo uni multicast-group-number enable** command to remove the configuration.

By default, a UNI does not remove the VLAN tag of the downlink multicast flow.

Examples

Remove the VLAN tag of the downlink multicast flow on UNI 1 of the ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 multicast-strip-tag enable
```

uni port-isolate

Syntax

uni *uni-number* **port-isolate**

undo uni *uni-number* **port-isolate**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni port-isolate** command to add a UNI to an isolation group.

Use the **undo uni port-isolate** command to remove a UNI from an isolation group.

Only one isolation group can be created on an ONU device.

By default, a UNI is not in any isolation group.

Caution

- This command takes effect on H3C ONUs only.
- A UNI port of an ET254-L ONU can be added to an isolation group only when the UNI port's VLAN operation mode is the transparent transmission mode.

Examples

Add UNI 1 and UNI 2 to the isolation group.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 port-isolate
[Sysname-Onu3/0/1:1] uni 2 port-isolate
```

uni restart auto-negotiation

Syntax

uni *uni-number* **restart auto-negotiation**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni restart auto-negotiation** command to force a UNI port to restart the auto-negotiation.

Note that this command takes effect only when auto-negotiation is enabled on the UNI port.

Examples

Force UNI 1 to restart the auto-negotiation.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 restart auto-negotiation
```

uni shutdown

Syntax

uni *uni-number* **shutdown**

undo uni *uni-number* **shutdown**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni shutdown** command to disable the UNIs.

Use the **undo uni shutdown** command to enable the UNIs.

By default, all the UNIs are disabled.

Examples

Disable UNI 1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 shutdown
```

uni speed

Syntax

uni *uni-number* **speed** { **10** | **100** | **auto** }

undo uni *uni-number* **speed**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

10: Specifies the port speed to 10 Mbps.

100: Specifies the port speed to 100 Mbps.

auto: Specifies the port speed to be auto-negotiated.

Description

Use the **uni** *uni-number* **speed** command to set the operating speed for a UNI.

Use the **undo uni** *uni-number* **speed** command to restore the default operating speed for a UNI.

By default, the operating speed of a UNI port is 100Mbps.

Caution

This command takes effect on H3C ONUs only.

Examples

Specify the speed for UNI 1 to 10 Mbps.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 speed 10
```

uni vlan-mode tag pvid

Syntax

uni *uni-number* **vlan-mode tag pvid** *pvid* [**priority** *priority-value*]

undo uni *uni-number* **vlan-mode**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of current ONU UNIs. The maximum number of UNI ports supported is 80.

Value: 802.1p precedence value of a packet, in the range of 0 to 7.

pvid: Default VLAN ID, in the range 1 to 4094.

Description

Use the **uni vlan-mode tag pvid** command to configure the VLAN operation mode of the specified UNI as the VLAN tag mode and set the related parameters.

Use the **undo uni vlan-mode** command to restore the default VLAN operation mode of the UNI.

By default, the VLAN operation mode of a UNI is VLAN transparent transmission mode.

Related command: **uni vlan-mode translation pvid**, **uni vlan-mode transparent**.

Caution

- If a UNI of an ET254-L ONU is added to an isolation group, the operation mode of the UNI port can be set to the transparent transmission mode only, but not VLAN tag mode or VLAN translation mode.
- If all ONU ports under an OLT port are access ports, to make sure that the packets received on the ONU port and PC are untagged packets, the VLAN operation mode of a UNI can only be configured as the transparent transmission mode.

Examples

Configure the VLAN operation mode of UNI 1 as VLAN tag mode, add the VLAN 100 tag to the untagged packets received on the port, and set the 802.1p precedence of the packets to 3.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] uni 1 vlan-mode tag pvid 100 priority 3
```

uni vlan-mode translation pvid

Syntax

uni *uni-number* **vlan-mode translation pvid** *pvid* [**priority** *priority-value*] { *oldvid* **to** *newvid* } *&<1-15>*

undo uni *uni-number* **vlan-mode**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

priority-value: 802.1p precedence for packets, in the range 0 to 7.

pvid: VLAN ID, in the range 1 to 4094.

oldvid: Original VLAN ID, in the range 1 to 4094.

newvid: New VLAN ID, in the range 1 to 4094.

&<1-15>: Means that you can specify up to 15 VLAN IDs for the corresponding argument.

Description

Use the **uni vlan-mode translation pvid** command to configure the VLAN operation mode of the specified UNI as the VLAN translation mode and set the related parameters.

Use the **undo uni vlan-mode** command to restore the default VLAN operation mode of the UNI.

By default, the VLAN operation mode of a UNI is VLAN transparent transmission mode.

Related commands: **uni vlan-mode tag pvid**, **uni vlan-mode transparent**.

Caution

- If a UNI port of an ET254-L ONU is added to an isolation group, the operation mode of the UNI port can be set to the transparent transmission mode only, but not VLAN tag mode or VLAN Translation mode.
- When all the ONU ports under an OLT port are Access ports, the operation mode of the UNI port can be set to the transparent transmission mode only to ensure the ONU ports and user PCs receive untagged packets.

Examples

Configure the VLAN operation mode of UNI 1 as VLAN translation mode, add the VLAN 100 tag to the untagged packets received on the port, map VLAN ID 2 to VLAN ID 5, and set the 802.1p precedence for the packets to 3.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] uni 1 vlan-mode translation pvid 100 priority 3 2 to 5
```

uni vlan-mode transparent

Syntax

uni *uni-number* **vlan-mode transparent**

undo uni *uni-number* **vlan-mode**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of current ONU UNIs. The maximum number of UNI ports supported is 80.

Description

Use the **uni vlan-mode transparent** command to configure the VLAN operation mode of a UNI as VLAN transparent transmission mode.

Use the **undo uni vlan-mode** command to restore the default VLAN operation mode of the UNI.

By default, the VLAN operation mode of a UNI is VLAN transparent transmission mode.

Related command: **uni vlan-mode tag pvid**, **uni vlan-mode translation pvid**.

Caution

- If a UNI port of an ET254-L ONU is added to an isolation group, the operation mode of the UNI port can be set to the transparent transmission mode only, but not VLAN tag mode or VLAN Translation mode.
- If all ONU ports under an OLT port are access ports, to make sure that the packets received on the ONU port and PC are untagged packets, the VLAN operation mode of a UNI can only be configured as the transparent mode.

Examples

Configure the VLAN operation mode of UNI 1 as VLAN transparent transmission mode.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] uni 1 vlan-mode transparent
```

upstream-sla

Syntax

upstream-sla { **minimum-bandwidth** *value1* | **maximum-bandwidth** *value2* | **delay** { **low** | **high** } } *

undo upstream-sla

View

ONU port view

Default Level

2: System level

Parameters

minimum-bandwidth *value1*: Specifies the minimum uplink bandwidth, in the unit of 64 kbps. *value1* is in the range 8 to 14400 and defaults to 32.

maximum-bandwidth *value2*: Specifies the maximum uplink bandwidth, in the unit of 64 kbps. *value2* is in the range 8 to 16000 and defaults to 368.

delay: Specifies the delay mode. The **low** keyword means that low delay is adopted and the **high** keyword is high delay. Low delay is adopted by default.

Description

Use the **upstream-sla** command to set the ONU's minimum uplink bandwidth, maximum uplink bandwidth, and delay mode of packet forwarding through the EPON system.

Use the **undo upstream-sla** command to restore the default values.

Caution

The sum of the minimum uplink bandwidths configured for all the created ONU ports under an OLT port cannot exceed 921600 kbps, namely, 900 Mbps.

Examples

Set the ONU port's minimum uplink bandwidth to 9600 kbps and maximum uplink bandwidth to 12800 kbps.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] upstream-sla minimum-bandwidth 150 maximum-bandwidth 200
 Info: The minimum-bandwidth of upstream is 9600 Kbps
 Info: The maximum-bandwidth of upstream is 12800 Kbps
```

update onu filename

Syntax

update onu filename *file-url*

undo update onu

View

OLT port view, ONU port view

Default Level

2: System level

Parameters

file-url: Update file name, a string of 1 to 64 characters composed of the device name and the ONU update file name. If no device name is specified, it is the name of the Flash of the SRPU. The files in the salve SRPU cannot be used for the update.

Description

Use the **update onu filename** command to remotely update ONU(s) by using the update file stored on the OLT.

Use the **undo update onu** command to cancel the remote ONU update configuration.

- Executing this command in OLT port view will update all the ONUs corresponding to the created ONUs under the OLT port.
- Executing this command in ONU port view will update the ONU corresponding to the ONU port.

Note that this is a configuration command. After it is configured in OLT port view or ONU port view, the update command will be executed on the corresponding ONU port:

- If the ONU corresponding to the ONU port is online and matches the update file, the ONU is updated directly.
- If the ONU corresponding to the ONU port is online but does not match the update file, the ONU cannot be updated.

- If the ONU corresponding to the ONU port is not online (because the ONU port is not bound with any ONU or the extended OAM connection fails on the bound ONU), the update process will not start until the ONU goes online.

Note

- After the update command is issued, the OLT will wait 15 to 20 seconds before executing the command. This allows for batch updating and saves system resources.
- The **update onu filename** command is a configuration command, that is, after the **update onu filename** command is executed, it will be saved in the configuration file of the device. If the ONU port corresponding to an ONU that goes online is created before the update command is used, the ONU will be updated directly (if it matches the update files). Otherwise, the ONU will not be updated. To update only the current ONUs online but not the offline ONUs or subsequently registered ONUs, execute the **update onu filename** command, and use the **undo update onu** command after you make sure that all online ONUs have been updated.
- Any power failure during the ONU software upgrade may cause update failure.
- Once the update file is transferred to the ONU, the ONU restarts automatically to complete the update.

Examples

Update an ONU.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] update onu filename file.app
Update flash:/file.app?[Y/N]
```

To start the upgrade, enter **Y**; to abort, enter **N**. The following example shows the output after you enter **Y**.

```
Info: Download file to onu may take a long time, please wait...
 Please wait while the firmware is being burnt, and check the software version after re-registration!
```

update onu onu-type

Syntax

update onu onu-type *onu-type* **filename** *file-url*

undo update onu onu-type *onu-type*

View

FTTH view

Default Level

2: System level

Parameters

onu-type: ONU type, a string of 1 to 16 case-insensitive characters, such as ET704-A and ET704-A-L.

file-url: Update file name, a string of 1 to 64 characters composed of the device name and the ONU update file name. If no device name is specified, it is the name of the Flash of the SRPU. The files in the salve SRPU cannot be used for the update.

Description

Use the **update onu onu-type** command to update ONUs by type.

Use the **undo update onu onu-type** command to cancel ONU update configuration by type.

Note that this is a configuration command. It takes effect only on the specified type of ONUs on which no update command is configured under the ONU port.

- If the ONU is online and matches the specified update file, the ONU is updated directly.
- If the ONU is online but does not match the update file, the update will fail.
- If the ONU is not online (because the ONU port is not bound with any ONU or the extended OAM connection fails on the bound ONU), the update process will not start until the ONU goes online.

Updating ONUs by type is recommended because it is efficient and easy-to-use.

Note

- After the update command is issued, the OLT will wait 15 to 20 seconds before executing the command. This allows for batch updating and saves system resources.
- The update configuration performed in port view takes precedence over that in FTTH view. For example, assume the ONU corresponding to ONU port ONU 3/0/1:1 is of type A. If you configure the update file for type A ONUs as **1.app** in FTTH view and configure the update file as **2.app** in ONU 3/0/1:1 port view, 2.app will be used to update the ONU.
- Any power failure during the ONU software upgrade may cause update failure.
- Once the update file is transferred to the ONU, the ONU restarts automatically to complete the update.
- An OLT can update up to 64 types of ONUs at the same time. That is, update files can be specified for up to 64 types of ONUs at the same time through the command line for updating ONUs by type.
- The **update onu onu-type** command is a configuration command, that is, after the **update onu onu-type** command is executed, it will be saved in the configuration file of the device. If the ONU port corresponding to an ONU that goes online is created before the update command is used, the ONU will be updated directly (if it matches the update files). Otherwise, the ONU will not be updated. To update only the current ONUs online but not the offline ONUs or subsequently registered ONUs, execute the **update onu onu-type** command, and use the **undo update onu onu-type** command after you make sure that all online ONUs have been updated.

Examples

Update all the ET704-A-L ONUs under the switch.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] update onu onu-type et704-a-l filename file.app
```

After the command is executed, the OLT starts updating all the ET704-A-L ONUs on which no update command is configured under the ONU port.

3 Alarm Configuration Commands

Note

- An alarm command executed in FTTH view will take effect on all the OLT ports of the system or all the ONUs under the OLT;
- An alarm command executed in OLT port view will take effect on the current port and all the ONUs under it;
- An alarm command executed in ONU port view will take effect only on the ONUs under the port.

Alarm Configuration Commands

alarm bit-error-rate

Syntax

alarm bit-error-rate { **direction** { **uplink** | **downlink** | **up-down-link** } | **threshold** *threshold* } *

undo alarm bit-error-rate { **direction** | **threshold** } *

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

uplink: Specifies the monitor direction. Only uplink data will be monitored.

downlink: Specifies the monitor direction. Only downlink data will be monitored.

up-down-link: Specifies the monitor direction. Both uplink and downlink data between OLT and ONU will be monitored.

threshold *threshold*: Specifies the alarm threshold of bit error rate. The *threshold* argument ranges from 1 to 10^9 and defaults to 10 (in 10^{-9}).

Description

Use the **alarm bit-error-rate** command to configure the monitor direction and the alarm threshold of the bit error rate.

Use the **undo alarm bit-error-rate** command to restore the default monitor direction and alarm threshold.

The system generates a bit error rate alarm when the total number of error bits or bit error rate of the data transferred between the OLT and ONUs exceeds the alarm threshold.

By default, both uplink and downlink data between OLT and ONU will be monitored.

Related commands: **alarm bit-error-rate enable**.

Examples

Configure OLT 1/0/1 to monitor only the uplink data between OLT and ONU, and set the alarm threshold of bit error rate to 20.

```
<Sysname> system-view
[Sysname] interface olt 1/0/1
[Sysname-Olt1/0/1] alarm bit-error-rate direction uplink threshold 20
```

alarm bit-error-rate enable

Syntax

alarm bit-error-rate enable

undo alarm bit-error-rate enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm bit-error-rate enable** command to enable the bit error rate alarm.

Use the **undo alarm bit-error-rate enable** command to disable the bit error rate alarm.

By default, the bit error rate alarm is enabled.

Examples

Enable the bit error rate alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm bit-error-rate enable
```

alarm device-fatal-error enable

Syntax

alarm device-fatal-error enable

undo alarm device-fatal-error enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm device-fatal-error enable** command to enable the device fatal error alarm.

Use the **undo alarm device-fatal-error enable** command to disable the device fatal error alarm.

By default, the device fatal error alarm is enabled.

When fatal errors occur to the device, the device fatal error alarm is generated. If the device does not detect the same error again within two minutes, the device fatal error alarm is removed.

Examples

Enable the device fatal error alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm device-fatal-error enable
```

alarm frame-error-rate

Syntax

alarm frame-error-rate { **direction** { **uplink** | **downlink** | **up-down-link**} | **threshold** *threshold* } *****

undo alarm frame-error-rate { **direction** | **threshold** } *****

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

uplink: Specifies the monitor direction. Only uplink data will be monitored.

downlink: Specifies the monitor direction. Only downlink data will be monitored.

up-down-link: Specifies the monitor direction. Both uplink and downlink data between OLT and ONU will be monitored.

threshold *threshold*: Specifies the alarm threshold of the frame error rate. The *threshold* argument ranges from 1 to 10^9 and defaults to 1 (in 10^{-9}).

Description

Use the **alarm frame-error-rate** command to configure the monitor direction and the alarm threshold of the frame error rate.

Use the **undo alarm frame-error-rate** command to restore the default monitor direction and alarm threshold.

When the total number of error frames and error frame rate of the data transferred between the OLT and ONU exceed the alarm thresholds, the frame error rate alarm occurs.

By default, both uplink and downlink data between OLT and ONU are monitored.

Related commands: **alarm frame-error-rate enable**.

Examples

Enable the frame error rate alarm on OLT 1/0/1, adopt the default monitor direction, and set the corresponding alarm threshold to 20.

```
<Sysname> system-view
[Sysname] interface olt 1/0/1
[Sysname-Olt1/0/1] alarm frame-error-rate direction up-down-link threshold 20
```

alarm frame-error-rate enable

Syntax

alarm frame-error-rate enable

undo alarm frame-error-rate enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm frame-error-rate enable** command to enable the frame error rate alarm.

Use the **undo alarm frame-error-rate enable** command to disable the frame error rate alarm.

By default, the frame error rate alarm is enabled.

Examples

Enable the frame error rate alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm frame-error-rate enable
```

alarm llid-mismatch enable

Syntax

alarm llid-mismatch enable

undo alarm llid-mismatch enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm llid-mismatch enable** command to enable the LLID mismatch frame alarm.

Use the **undo alarm llid-mismatch enable** command to disable the LLID mismatch frame alarm.

By default, the LLID mismatch frame alarm is disabled.

Examples

Enable the LLID mismatch frame alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm llid-mismatch enable
```

alarm llid-mismatch threshold

Syntax

alarm llid-mismatch threshold *threshold*

undo alarm llid-mismatch threshold

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

threshold *threshold*: Specifies the alarm threshold of the LLID mismatch frame alarm. It ranges from 1000 to 10^9 frames and defaults to 5000 frames.

Description

Use the **alarm llid-mismatch threshold** command to configure the alarm threshold of LLID mismatch frame.

Use the **undo alarm llid-mismatch threshold** command to restore the default alarm threshold.

The system generates an LLID mismatch frame alarm when the timeslots are used in disorder, that is, one ONU uses another ONU's timeslot to forward data.

Related commands: **alarm llid-mismatch enable**.

Examples

Set the alarm threshold of LLID mismatch frame to 6000 frames.

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

```
[Sysname-Olt1/0/1] alarm llid-mismatch threshold 6000
```

alarm local-stable enable

Syntax

alarm local-stable enable

undo alarm local-stable enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm local-stable enable** command to enable the local stable alarm.

Use the **undo alarm local-stable enable** command to disable the local stable alarm.

The system generates a local stable alarm in case of an ONU misuse in the system, for example, when an OAM 2.0 ONU and an OAM 3.3 ONU are mixed in the same system. (All ONUs in the same system must adopt the same OAM version.)

The local stable alarm differs from the remote stable alarm in the following ways:

- The local stable alarm is generated at the OLT side.
- The remote stable alarm is generated at the ONU side and will be reported to the OLT.

By default, this function is enabled.

Related commands: **alarm remote-stable**.

Examples

Enable the local stable alarm OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm local-stable enable
```

alarm oam critical-event enable

Syntax

alarm oam critical-event enable

undo alarm oam critical-event enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam critical-event enable** command to enable the critical event alarm.

Use the **undo alarm oam critical-event enable** command to disable the critical event alarm.

By default, the critical event alarm is enabled.

There are two types of critical events: local link fault and dying gasp. The system generates a critical event alarm when one of the two events occurs.

Examples

Enable the critical event alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm oam critical-event enable
```

alarm oam dying-gasp enable

Syntax

alarm oam dying-gasp enable

undo alarm oam dying-gasp enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam dying-gasp enable** command to enable the dying gasp alarm.

Use the **undo alarm oam dying-gasp enable** command to disable the dying gasp alarm.

By default, the dying gasp alarm is enabled.

The system generates a dying gasp alarm when a system error, a data loading error or any other nonreversible errors occurs.

Examples

Enable the dying gasp alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
```

```
[Sysname-Olt3/0/1] alarm oam dying-gasp enable
```

alarm oam error-symbol-period

Syntax

alarm oam error-symbol-period { **window-high** *windowhigh* | **window-low** *windowlow* | **threshold-high** *thresholdhigh* | **threshold-low** *thresholdlow* } ***

undo alarm oam error-symbol-period { **window-high** | **window-low** | **threshold-high** | **threshold-low** } ***

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

window-high *windowhigh*: Specifies the higher window size, in the range 0 to 4,294,967,295 (2^{32}-1). By default, the higher window size is 0.

window-low *windowlow*: Specifies the lower window size, in the range 0 to 4,294,967,295 (2^{32}-1). By default, the lower window size is 1.

threshold-high *thresholdhigh*: Specifies the higher alarm threshold, in the range 0 to 4,294,967,295 (2^{32}-1). By default, the higher alarm threshold is 0.

threshold-low *thresholdlow*: Specifies the lower alarm threshold, in the range 0 to 4,294,967,295 (2^{32}-1). By default, the lower alarm threshold is 20.

Note

- The window size and threshold values specified in this command comprise two parts, the higher part and the lower part, both of which are 16 bits in length.
- By default, the window size is 1 second, and the threshold is 20 bytes.

Description

Use the **alarm oam error-symbol-period** command to configure the corresponding window size and alarm threshold.

Use the **undo alarm oam error-symbol-period** command to restore the default window size and alarm threshold.

The system generates an error symbol period alarm when the number of error bytes in a specific period (that is, the window size) exceeds the corresponding predefined threshold.

Related commands: **alarm oam error-symbol-period enable**.

Caution

- When the upper limit and the lower limit of the alarm threshold are set to 0, large amount of alarms are generated immediately. Since alarm events are carried in the OAM packets, large amount of OAM packets are generated. In this case, OAM packets may be lost.
- The commands here take effect only for OAM 2.0 and above.

Examples

On ONU 1/0/1:1, set the higher window size, lower window size, higher alarm threshold, and lower alarm threshold for the error symbol period alarm to 1, 3, 10, and 30 respectively.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] alarm oam error-symbol-period window-high 1 window-low 3 threshold-high 10 threshold-low 30
```

alarm oam error-symbol-period enable

Syntax

alarm oam error-symbol-period enable

undo alarm oam error-symbol-period enable

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam error-symbol-period enable** command to enable the error symbol period alarm.

Use the **undo alarm oam error-symbol-period enable** command to disable the error symbol period alarm.

By default, the error symbol period alarm is enabled.

Caution

The commands here take effect only for OAM 2.0 and above.

Examples

Enable the error symbol period alarm on ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] alarm oam error-symbol-period enable
```

alarm oam error-frame-period

Syntax

alarm oam error-frame-period { **window** *window* | **threshold** *threshold* } *

undo alarm oam error-frame-period { **window** | **threshold** } *

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

window *window*: Specifies the window size, in the range 0 to 4294967295 (2^{32}-1) seconds. By default, the window size is 1 second.

threshold *threshold*: Specifies the alarm threshold, in the range 1 to 4294967295 (2^{32}-1) frames. By default, the threshold is 20 frames.

Description

Use the **alarm oam error-frame-period** command to configure the corresponding window size and alarm threshold.

Use the **undo alarm oam error-frame-period** command to restore the default window size and alarm threshold.

The system generates an error frame period alarm when the number of error frames in a specific time period (that is, the window size) exceeds the corresponding predefined threshold.

Related commands: **alarm oam error-frame-period enable**.

Caution

- When the alarm threshold is set to 0, large amount of alarms are generated immediately. Since alarm events are carried in the OAM packets, large amount of OAM packets are generated. In this case, OAM packets may be lost.
- The commands here take effect only for OAM 2.0 and above.

Examples

Set the window size and alarm threshold for error frame period to 2 seconds and 30 frames on ONU 1/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] alarm oam error-frame-period window 2 threshold 30
```

alarm oam error-frame-period enable

Syntax

alarm oam error-frame-period enable

undo alarm oam error-frame-period enable

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam error-frame-period enable** command to enable the error frame period alarm.

Use the **undo alarm oam error-frame-period enable** command to disable the error frame period alarm.

By default, the error frame period alarm is enabled.

 **Caution**

The commands here take effect only for OAM 2.0 and above.

Examples

Enable the error frame period alarm for the ONU corresponding to ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] alarm oam error-frame-period enable
```

alarm oam error-frame

Syntax

alarm oam error-frame { **window** *window* | **threshold** *threshold* } ***

undo alarm oam error-frame { **window** | **threshold** } ***

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

window *window*: Specifies the window size, in the range 0 to 65535 seconds. By default, the window size is 10 seconds.

threshold *threshold*: Specifies the alarm threshold, in the range 1 to 4294967295 (2^{32}-1) frames. By default, the threshold is 20 frames.

Description

Use the **alarm oam error-frame** command to configure the corresponding window size and alarm threshold.

Use the **undo alarm oam error-frame** to restore the default window size and alarm threshold.

The system generates an error frame alarm when the number of error frames in a specific time period (that is, the window size) exceeds the corresponding predefined threshold.

Related commands: **alarm oam error-frame enable**.

Caution

- When the alarm threshold is set to 0, large amount of alarms are generated immediately. Since alarm events are carried in the OAM packets, large amount of OAM packets are generated. In this case, OAM packets may be lost.
- The commands here take effect only for OAM 2.0 and above.

Examples

Set the window size and alarm threshold for error frame to 20 seconds and 30 frames on ONU 1/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] alarm oam error-frame window 20 threshold 30
```

alarm oam error-frame enable

Syntax

alarm oam error-frame enable

undo alarm oam error-frame enable

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam error-frame enable** command to enable the error frame alarm.

Use the **undo alarm oam error-frame enable** command to disable the error frame alarm.

By default, this function is enabled.

Caution

The commands here take effect only for OAM 2.0 and above.

Examples

Enable the error frame alarm for the ONU corresponding to ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] alarm oam error-frame enable
```

alarm oam error-frame-seconds-summary

Syntax

alarm oam error-frame-seconds-summary { **window** *window* | **threshold** *threshold* } *

undo alarm oam error-frame-seconds-summary { **window** | **threshold** } *

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

window *window*: Specifies the window size, in the range 100 to 9000 (in 100 ms). By default, the window size is 600.

threshold *threshold*: Specifies the alarm threshold, in the range 1 to 900 (in seconds). By default, the threshold is 1 second.

Description

Use the **alarm oam error-frame-seconds-summary** command to configure the corresponding window size and alarm threshold.

Use the **undo alarm oam error-frame-seconds-summary** to restore the default window size and alarm threshold.

The system generates an error frame seconds summary alarm when the number of error frame seconds (in an error frame second, at least one error frame occurs) in a specific time period (for example, 1 minute) exceeds the corresponding predefined threshold.

Related commands: **alarm oam error-frame-seconds-summary enable**.

Caution

The commands here take effect only for OAM 2.0 and above.

Examples

Set the window size and alarm threshold for error frame seconds summary to 800 and 2 on ONU 1/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 1/0/1:1
[Sysname-Onu1/0/1:1] alarm oam error-frame-seconds-summary window 800 threshold 2
```

alarm oam error-frame-seconds-summary enable

Syntax

alarm oam error-frame-seconds-summary enable

undo alarm oam error-frame-seconds-summary enable

View

OLT port view, ONU port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam error-frame-seconds-summary enable** command to enable the error frame seconds summary alarm.

Use the **undo alarm oam error-frame-seconds-summary enable** command to disable the error frame seconds summary alarm.

By default, the error frame seconds summary alarm is enabled.

Caution

The commands here take effect only for OAM 2.0 and above.

Examples

Enable the error frame seconds summary alarm for the ONU corresponding to ONU 3/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] alarm oam error-frame-seconds-summary enable
```

alarm oam local-link-fault enable

Syntax

alarm oam local-link-fault enable

undo alarm oam local-link-fault enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam local-link-fault enable** command to enable the local link fault alarm.

Use the **undo alarm oam local-link-fault enable** command to disable the local link fault alarm.

By default, the local ink fault alarm is enabled.

The system generates a local link fault alarm when the receiving direction of the local data terminal is in trouble.

Examples

Enable the local link fault alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm oam local-link-fault enable
```

alarm oam-vendor-specific enable

Syntax

alarm oam-vendor-specific enable

undo alarm oam-vendor-specific enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm oam-vendor-specific enable** command to enable the oam vendor specific alarm.

Use the **undo alarm oam-vendor-specific enable** command to disable the oam vendor specific alarm.

This alarm is customized by a vendor.

By default, the oam vendor specific alarm is enabled.

Examples

Enable the oam vendor specific alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm oam-vendor-specific enable
```

alarm onu-over-limitation enable

Syntax

alarm onu-over-limitation enable

undo alarm onu-over-limitation enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm onu-over- limitation enable** command to enable ONU over limitation alarm.

Use the **undo alarm onu-over- limitation enable** command to disable ONU over limitation alarm.

When the total number of ONUs connected to an OLT exceeds the limit, an alarm is generated.

By default, the onu over limitation alarm is enabled.

Examples

Enable the onu over limitation alarm on OLT 3/0/1.

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

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm onu-over-limitation enable
```

alarm port bit-error-rate enable

Syntax

alarm port bit-error-rate enable

undo alarm port bit-error-rate enable

View

ONU port view, OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm port bit-error-rate enable** command to enable the port bit error rate alarm.

Use the **undo alarm port bit-error-rate enable** command to disable the port bit error rate alarm.

When both the total number of error bits and bit error rate of the data transferred between the OLT and ONU exceed the alarm thresholds, the port bit error rate alarm occurs.

The threshold setting of the port bit error rate alarm is the same as that of the bit error rate alarm.

Related commands: **alarm bit-error-rate**.

By default, the port bit error rate alarm is enabled.

Examples

Enable the port bit error rate alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt3/0/1
[Sysname-Olt3/0/1] alarm port bit-error-rate enable
```

alarm registration-error enable

Syntax

alarm registration-error enable

undo alarm registration-error enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm registration-error enable** command to enable the registration error alarm.

Use the **undo alarm registration-error enable** command to disable the registration error alarm.

The system generates a registration error alarm when an error occurs during the registration of an ONU.

By default, the registration error alarm is enabled.

Examples

Enable the registration error alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt3/0/1
[Sysname-Olt3/0/1] alarm registration-error enable
```

alarm remote-stable enable

Syntax

alarm remote-stable enable

undo alarm remote-stable enable

View

OLT port view, FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm remote-stable enable** command to enable the remote stable alarm.

Use the **undo alarm remote-stable enable** command to disable the remote stable alarm.

The system generates a remote stable alarm in case of an ONU misuse in the system, for example, when an OAM 2.0 ONU and an OAM 3.3 ONU are mixed in the same system. (All ONUs in the same system must adopt the same OAM version.)

The local stable alarm differs from the remote stable alarm in the following way:

- The local stable alarm is generated at the OLT side.
- The remote stable alarm is generated at the ONU side and will be reported to the OLT.

By default, the remote stable alarm is enabled.

Related commands: **alarm local-stable**.

Examples

Enable the remote stable alarm on OLT 3/0/1.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] alarm remote-stable enable
```

alarm software-error enable

Syntax

alarm software-error enable

undo alarm software-error enable

View

FTTH view

Default Level

2: System level

Parameters

None

Description

Use the **alarm software-error enable** command to enable the software error alarm of the system.

Use the **undo alarm software-error enable** command to disable the software error alarm of the system.

The system generates a software error alarm when a signal error, DA abnormity (that is, data access abnormity) error, or memory allocation failure occurs.

By default, the software error alarm is enabled.

Examples

Enable the software error alarm in the EPON system.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] alarm software-error enable
```

monitor enable

Syntax

monitor enable

undo monitor enable

View

FTTH view

Default Level

3: Manage level

Parameters

None

Description

Use the **monitor enable** command to enable alarm monitor in the EPON system.

Use the **undo monitor enable** command to disable alarm monitor in the EPON system.

By default, alarm monitor is enabled in the EPON system.

Examples

Enable the alarm monitor of the EPON system

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] monitor enable
```

sample enable

Syntax

sample enable

undo sample enable

View

FTTH view

Default Level

3: Manage level

Parameters

None

Description

Use the **sample enable** command to enable system statistics sampling.

Use the **undo sample enable** command to disable system statistics sampling.

By default, system statistics sampling is enabled.

Examples

Enable statistics sampling in the EPON system.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] sample enable
```

timer monitor

Syntax

timer monitor *seconds*

undo timer monitor

View

FTTH view

Default Level

3: Manage level

Parameters

seconds: Alarm monitor period, ranging from 1 to 3600 (in seconds). The system default is 80 seconds.

Description

Use the **timer monitor** command to configure the alarm monitor period of the system.

Use the **undo timer monitor** command to restore the default monitor period.

Examples

Configure the alarm monitor period of the EPON system to 100 seconds.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] timer monitor 100
```

timer sample

Syntax

timer sample *seconds*

undo timer sample

View

FTTH view

Default Level

3: Manage level

Parameters

seconds: Sampling interval (in seconds). It is in the range 1 to 3600 and defaults to 4.

Description

Use the **timer sample** command to set the sampling interval for the system.

Use the **undo timer sample** command to restore the default sampling interval for the system.

Examples

Set the sampling interval of the EPON system to 10 seconds.

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] timer sample 10
```

4 Switch Feature-Related Configuration Commands

OLT Port Configuration Commands

Table 4-1 OLT port features

Feature	Command	Related section
Basic parameters	• **description** • **shutdown** • **interface** • **display interface**	Ethernet interface commands
Flow control	• **flow-control**	Ethernet interface commands
Broadcast storm suppression	• **broadcast-suppression** • **multicast-suppression** • **unicast-suppression**	Ethernet interface commands
Port isolation	• **port-isolate enable** • **display port-isolate group**	Port isolation configuration
Port Trap	**enable snmp trap updown**	SNMP commands
IGMP Snooping	**igmp-snooping source-deny**	IGMP Snooping commands
MLD Snooping	**mld-snooping source-deny**	MLD Snooping commands
QinQ	• **qinq enable** • **qinq enable downlink** • **qinq enable uplink** • **qinq ethernet-type service-tag**	QinQ / VLAN Mapping commands
Port mirroring	• **display mirroring-group** • **mirroring-group mirroring-port** • **mirroring-group monitor-port** • **mirroring-group monitor-egress** • **mirroring-port** • **monitor-port**	Port mirroring commands
802.1X feature	• **display dot1x** • **dot1x** • **dot1x handshake** • **dot1x max-user** • **dot1x port-control { authorized-force | auto | unauthorized-force }** • **dot1x supp-proxy-check { logoff | trap }** • **dot1x multicast-trigger** • **reset dot1x statistics**	802.1X commands

Feature	Command	Related section
MAC authentication	• **display mac-authentication** • **mac-authentication** • **reset mac-authentication statistics**	MAC authentication commands
IP Source Guard	• **display ip check source** • **display user-bind** • **ip check source** • **user-bind**	IP Source Guard commands
QoS	• **bandwidth downstream priority-queue** • **priority-queue-mapping** • **qos gts** • **qos lr** • **qos apply policy** • **qos sp** • **qos wrr** • **qos wfq** • **qos wred** • **qos priority** • **qos trust** • **display qos gts interface** • **display qos lr interface** • **display qos policy interface** • **display qos sp interface** • **display qos wrr interface** • **display qos wfq interface** • **display qos wred interface** • **display qos trust interface**	QoS commands
Smart Link	**smart-link flush enable** [**control-vlan** *vlan-id*]	Smart Link commands

Caution

- When an up OLT port goes down (because the **shutdown** is executed on it or the fiber is unplugged), wait at least five seconds before bringing up the port again (by using the **undo shutdown** command or plugging in the fiber). This will prevent the anomalies caused by frequent ONU registrations and deregistrations.
- Currently, the **qinq enable downlink** and **qinq enable uplink** commands are not supported on an OLT port.

ONU Port Configuration Commands

Table 4-2 ONU port features

Feature	Command	Related section
Basic parameters	• **description** • **shutdown** • **link-delay** • **interface** • **display interface** • **reset counters interface**	Ethernet interface commands
Loopback test	**loopback**	Ethernet interface commands
Port Trap	**enable snmp trap updown**	SNMP commands
MAC address table management	• **mac-address** • **mac-address max-mac-count** • **display mac-address** • **display mac-address mac-learning**	MAC address table management commands
DHCP Snooping	• **dhcp-snooping information enable** • **dhcp-snooping information format** • **dhcp-snooping information strategy** • **dhcp-snooping information circuit-id format-type** • **dhcp-snooping information circuit-id string** • **dhcp-snooping information remote-id format-type** • **dhcp-snooping information remote-id string**	DHCP commands
IGMP Snooping	• **igmp-snooping fast-leave** • **igmp-snooping group-limit** • **igmp-snooping group-policy** • **igmp-snooping host-join** • **igmp-snooping overflow-replace** • **igmp-snooping static-group** • **igmp-snooping static-router-port**	IGMP Snooping commands
MLD Snooping	• **mld-snooping fast-leave** • **mld-snooping group-limit** • **mld-snooping group-policy** • **mld-snooping host-join** • **mld-snooping overflow-replace** • **mld-snooping static-group** • **mld-snooping static-router-port**	MLD Snooping commands

Feature	Command	Related section
QoS	• **bandwidth downstream** • **bandwidth downstream high-priority enable** • **bandwidth downstream policy enable** • **qos apply policy** • **qos cos-local-precedence-map** • **qos sp** • **qos wrr** • **qos wfq** • **qos priority** • **qos trust** • **uni classification-marking** • **uni port-policing** • **display qos policy interface** • **display qos sp interface** • **display qos trust interface** • **display qos wrr interface** • **display qos wfq interface**	QoS commands
Port mirroring	• **uni mirroring-port** • **uni monitor-port**	Port mirroring commands
802.1X feature	• **display dot1x** • **dot1x** • **dot1x guest-vlan** • **dot1x handshake** • **dot1x max-user** • **dot1x port-control** { **authorized-force | auto | unauthorized-force** } • **dot1x supp-proxy-check** { **logoff | trap** } • **dot1x multicast-trigger** • **reset dot1x statistics**	802.1X commands

Note

In an EPON system, users and the multicast source can exchange multicast traffic with each other only if the corresponding multicast table entries exist on the ONUs and OLT:

- In FTTH view, bind multicast IP addresses with multicast VLANs. Then, the multicast table entries will be created on the ONUs and OLT when users send IGMP report messages.
- You can use the **igmp-snooping host-join** and **igmp-snooping static-group** commands in ONU port view to create multicast table entries on the OLT, but not on the ONUs. In that case, multicast traffic cannot be exchanged between them.

Table of Contents

1 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.

When you carry out this command, MSTP will replace the currently running MST region–related parameters with the parameters you have just configured, and will perform spanning tree calculation again.

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

Examples

Activate MST region configuration manually.

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

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 all the configuration information of the MST region, including the region name, VLAN-to-MSTI mapping and revision level settings.

Be sure that your MST region configurations are correct, especially the VLAN-to-MSTI mapping table. As defined in the MSTP protocol, MSTP-enabled devices are in the same MST region only when they have the same format selector (protocol format selector defined in 802.1s, which is 0 by default and unconfigurable), region name, VLAN-to-MSTI mapping table, and MSTP revision level settings. A device will be in a different region if it is different in any of these four settings.

You can view all the MST region–related configuration information by using this command and determine the MST region the device is currently in, or check whether the MST region configuration is correct.

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

Examples

View all the configuration information of the MST region.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
   Format selector :0
   Region name     :00b010000001
   Revision level  :0

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

Table 1-1 check region-configuration command output description

Field	Description
Format selector	Configuration format selector of the MST region
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-MSTI 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 spanning tree information of a particular MSTI. The value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the common internal spanning tree (CIST).

interface *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 &<1-10> indicates that you can specify up to 10 ports or port ranges.

slot *slot-number*: Displays the spanning tree information of the card on the specified slot.

brief: Displays brief information.

Description

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

Based on the MSTP status information 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 ID or port list, this command will display the MSTP information on all ports. The displayed information is sequenced by MSTI ID and by port name in each MSTI.
- If you specify an MSTI ID, this command will display the MSTP information on all ports in that MSTI. The displayed information is sequenced by port name.
- If you specify a port list, this command will display the MSTP information on the specified ports. The displayed information is sequenced 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 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 (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 information and statistics information.

```
<Sysname> display stp instance 0 interface GigabitEthernet 2/0/1 to GigabitEthernet 2/0/4
brief
  MSTID      Port                 Role  STP State     Protection
   0     GigabitEthernet2/0/1      DESI  FORWARDING      NONE
   0     GigabitEthernet2/0/2      DESI  FORWARDING      NONE
   0     GigabitEthernet2/0/3      DESI  FORWARDING      NONE
   0     GigabitEthernet2/0/4      DESI  FORWARDING      NONE
```

Table 1-2 display stp command output description

Field	Description
MSTID	MSTI ID in the MST region
Port	Port name, corresponding to each MSTI
Role	Port role
STP State	MSTP status on the port, including forwarding, discarding, and learning
Protection	Protection type on the port, including root guard, loop guard, and BPDU guard

View the detailed MSTP status information and statistics information.

```
<Sysname> display stp instance 0 interface GigabitEthernet 2/0/2
----[CIST][Port198(GigabitEthernet2/0/2)][DOWN]----
 Port Protocol       :enabled
 Port Role           :CIST Disabled Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200000
 Desg. Bridge/Port   :32768.000f-e25d-f8ad / 128.198
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=false
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :0
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
 BPDU Sent           :0
          TCN: 0, Config: 0, RST: 0, MST: 0
```

```
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

Table 1-3 display stp command output description

Field	Description
Port Protocol	STP enable state of 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
Protection Type	Protection type on the port, including root guard and loop guard
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.
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI
PortTimes	Timer settings of the port, including Hello time, Max Age, Forward delay, Message Age, and Remain Hop
BPDU Sent	Statistics on sent BPDUs
BPDU Received	Statistics on received BPDUs

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 action
- Loop guard action
- MSTP BPDU format compatibility protection action

Examples

View information about abnormally blocked ports.

```
<Sysname> display stp abnormal-port
MSTID       Blocked Port                    Reason
1          GigabitEthernet2/0/1             ROOT-Protected
2          GigabitEthernet2/0/2             LOOP-Protected
2          GigabitEthernet2/0/3             Formatcompatibility-Protected
```

Table 1-4 display stp abnormal-port command output description

Field	Description
MSTID	MSTI ID
Blocked Port	Name of a blocked port, which corresponds to the related MSTI
Reason	Reason that caused abnormal blocking of the port. • ROOT-Protected: root guard action • LOOP-Protected: loop guard action • Formatcompatibility-Protected: MSTP BPDU format compatibility protection action

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 view the information about ports blocked by STP protection actions.

These actions include:

- BPDU attack guard action
- MSTP BPDU format compatibility protection action

Examples

View the information about ports blocked by STP protection actions.

```
<Sysname> display stp down-port
Down Port               Reason
GigabitEthernet2/0/1    BPDU-Protected
GigabitEthernet2/0/2    Formatfrequency-Protected
```

Table 1-5 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 action • Formatfrequency-Protected: MSTP BPDU format compatibility protection action

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 value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

slot *slot-number*: Displays the historic port role calculation information of the card on the specified slot.

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 sequenced 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 card on slot 1 in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
 --------------- STP slot 1 history trace ---------------
 -------------------  Instance 2   ---------------------
     Port GigabitEthernet2/0/1
       Role change   : ROOT->DESI (Aged)
       Time          : 2006/08/08 00:22:56
       Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

     Port GigabitEthernet2/0/2
       Role change   : ALTER->ROOT
       Time          : 2006/08/08 00:22:56
       Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Table 1-6 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-MSTI mappings.

Related commands: **stp region-configuration**.

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 1-7 display stp region-configuration command output description

Field	Description
Format selector	MSTP-defined format selector
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-MSTI 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        0.0013.1923.da80         0              0
```

Table 1-8 display stp root command output description

Field	Description
MSTID	MSTI ID
Root Bridge ID	Root bridge ID
ExtPathCost	External path cost
IntPathCost	Internal path cost
Root Port	Root port name (displayed only if a port of the current device is the root port of multiple 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 BPDUs (also known as TCN BPDUs) received and sent by all ports in a particular spanning tree instance. The value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

slot *slot-number*: Displays the statistics of TC BPDUs received and sent by all ports on a particular card.

Description

Use the **display stp tc** command to view the statistics of TC BPDUs received and sent.

Note that:

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

Examples

View the statistics of TC BPDUs received and sent by all ports on the card on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MSTID      Port                        Receive      Send
   0        GigabitEthernet2/0/1           6          4
   0        GigabitEthernet2/0/2           0          2
```

Table 1-9 display stp tc command output description

Field	Description
MSTID	MSTI ID in the MST region
Port	Port name
Receive	Number of TC BPDUs received on each port
Send	Number of TC 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, ranging from 0 to 31. The minimum value is 0, representing the CIST.

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 sub-VLAN ID and ranges from 1 to 4094. *&<1-10>* indicates you can specify up to 10 sub-VLAN IDs or sub-VLAN ID ranges.

Description

Use the **instance** command to map the specified VLAN(s) to the specified MSTI.

Use the **undo instance** command to remap the specified VLAN(s) 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.

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

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.

The MST region name, the VLAN-to-MSTI mapping table and the MSTP revision level of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **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 an Ethernet 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 port(s) (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 port(s) 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 2/0/1 through GigabitEthernet 2/0/3.

```
<Sysname> reset stp interface GigabitEthernet 2/0/1 to GigabitEthernet 2/0/3
```

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. The system default is 0.

Description

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

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

The MSTP revision level, the MST region name and the VLAN-to-MSTI mapping table of a device jointly determine the MST region the device belongs to.

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

Syntax

stp { **enable** | **disable** }

undo stp

View

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

Default Level

2: System level

Parameters

enable: Enables the MSTP feature.

disable: Disables the MSTP feature.

Description

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

Use the **undo stp** command to restore the default MSTP status.

By default, MSTP is disabled globally. When you enable MSTP globally, it is enabled automatically on all the ports on the device.

Note that:

- To control MSTP flexibly, you can disable the MSTP feature for certain ports so that they will not take part in spanning tree calculation and thus to save the device's CPU resources.
- After you enable MSTP, the device determines whether to work in STP-compatible mode, in RSTP mode or in MSTP mode according to your MSTP work mode setting. After MSTP is disabled, the device becomes a transparent bridge.
- After being enabled, MSTP dynamically maintains spanning tree status of the corresponding VLANs based on the received configuration BPDUs. After being disabled, it stops maintaining the spanning tree status.
- Configured in system view, the setting takes effect for the device globally; configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **stp mode**.

Examples

Enable the MSTP feature globally.

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

Disable MSTP on port GigabitEthernet 2/0/1.

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

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp disable
```

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 for the device.

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

By default, the BPDU guard function is disabled.

Examples

Enable the BPDU guard function for the device.

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

stp bridge-diameter

Syntax

stp bridge-diameter *bridge-number*

undo stp bridge-diameter

View

System view

Default Level

2: System level

Parameters

bridge-number: 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.

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.

Note that this configuration is effective for the CIST and root bridge only, and 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 port view, port group view, Layer-2 aggregate port 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 port(s) will use to recognize and send MSTP BPDUs.

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

The default mode is **auto**, namely all ports recognize the BPDU format automatically.

Note that:

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

port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

- If the mode is set to **auto** on a port, the port automatically recognizes and resolves the received compatible-format BPDUs or 802.1s-compliant BPDUs, and sends, when needed, compatible-format or 802.1s-compliant BPDUs.
- If the mode is set to **legacy** or **dot1s** on a port, the port can only receive and send BPDUs of the specified format. If the port is configured not to detect the packet format automatically while it works in the MSTP mode, and if it receives a packet in the format other than the configured format, it will become a designated port and remain in the discarding state to prevent the occurrence of a loop.

Examples

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

```
<Sysname>system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp compliance dot1s
```

Restore the default mode for port Ethernet 1/1 to recognize and send MSTP BPDUs.

```
[Sysname-GigabitEthernet2/0/1] undo stp compliance
```

stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

View

System view, Ethernet port view, port group view, Layer-2 aggregate port 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 port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

- You need to enable this feature both globally and on ports connected to other vendors' 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, and disable the feature globally to disable it on all associated ports.
- It is not recommended to enable Digest Snooping on the MST region edge ports to avoid loops.

Examples

Enable Digest Snooping globally.

```
<Sysname> system-view
[Sysname] stp config-digest-snooping
```

Enable Digest Snooping on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp config-digest-snooping
```

stp cost

Syntax

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

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

View

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

Default Level

2: System level

Parameters

instance *instance-id*: Sets the path cost of the port(s) in a particular MSTI. The value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

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 proprietary 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.

- Configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If you set *instance-id* to 0, you are setting the path cost of the port in the CIST. The path cost setting of a port can affect the role selection of the port. Setting different path costs for the same port in different MSTIs allows different VLAN traffic flows to be forwarded along different physical links, thus to enable VLAN-based load balancing. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples

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

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp instance 2 cost 200
```

stp edged-port

Syntax

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

undo stp edged-port

View

Ethernet port view, port group view, Layer-2 aggregate port 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) to be an edge port or edge ports.

Use the **stp edged-port disable** or **undo stp edged-port enable** command to configure the port(s) to be a non-edge port or non-edge ports.

All Ethernet ports are non-edge ports by default.

Note that:

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

port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

- 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 an Ethernet 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 2/0/1 as a non-edge port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp edged-port disable
```

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

Ethernet port view, port group view, Layer-2 aggregate port 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 port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Enable the loop guard function on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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.

By default, the maximum number of hops of an MST region is 20.

The maximum hops configured in an MST region limit the size of the MST region. In an MST region, the maximum hops configured on the regional root bridge are the maximum hops of this MST region. After a configuration BPDU leaves the root bridge, its hop count is decremented by 1 each time it passes a device. When its hop count reaches 0, it will be discarded by the device that received it. As a result, devices beyond the maximum hop count are unable to take part in spanning tree calculation, and thereby the size of the MST region is limited.

Devices other than the root bridge in an MST region use the maximum hops setting on the root bridge.

Examples

Set the maximum hops of the MST region to 35.

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

stp mcheck

Syntax

stp mcheck

View

System view, Ethernet port view, Layer-2 aggregate port 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.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, the port will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that:

- The **stp mcheck** command is meaningful only when the device works in the MSTP (or RSTP-compatible) mode, not in the STP-compatible mode.
- Configured in system view, the setting takes effect globally; configured in port view, the setting takes effect on the current port only.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **stp mode**.

Examples

Carry out mCheck on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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**.

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 port view, port group view, Layer-2 aggregate port 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 port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Note

The No Agreement Check feature can take effect only on the root port.

Examples

Enable No Agreement Check on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 proprietary 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 **legacy** standard is used for calculating the default path cost for ports.

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 1-10 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 proprietary 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

When calculating path cost for an aggregate port, 802.1D-1998 does not take into account the number of member ports in its aggregation group as 802.1T does. The calculation formula 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.

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
```

Configure the device to calculate the default path cost for ports based on IEEE 802.1t.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1t
```

stp point-to-point

Syntax

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

undo stp point-to-point

View

Ethernet port view, port group view, Layer-2 aggregate port 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 specify whether the current port(s) is/are connected to a point-to-point link or point-to-point links.

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 an Ethernet port connects to a point-to-point link.

Note that:

- Configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- 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 port 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.

Examples

Configure port GigabitEthernet 2/0/3 as connecting to a point-to-point link.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/3
[Sysname-GigabitEthernet2/0/3] 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 port view, port group view, Layer-2 aggregate port view

Default Level

2: System level

Parameters

instance *instance-id*: Sets the priority of the current port(s) in a particular spanning tree instance. The value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

priority: Port priority, in the range of 0 to 240 in steps 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.

By default, the port priority is 128.

Note that:

- Configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If you set *instance-id* to 0, you are setting the priority of the port in the CIST. The priority of a port can affect the role selection of the port in the specified MSTI.
- Setting different priorities for the same port in different MSTIs allows different VLAN traffic flows to be forwarded along different physical links, thus to enable 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.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST only.

Examples

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

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/3
[Sysname-GigabitEthernet2/0/3] 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 value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

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.

By default, this function is enabled.

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 GigabitEthernet 2/0/1 has been set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PFWD: Instance 2's GigabitEthernet 2/0/2 has been set to forwarding state!
```

// The information above shows that in MSTI 2 the state of GigabitEthernet 2/0/1 has changed to discarding and that of GigabitEthernet 2/0/2 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 particular spanning tree instance. The value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

priority: Port priority, in the range of 0 to 61440 in steps of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192…, on the device.

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.

The device priority is involved in spanning tree calculation. The device priority is set on a per-MSTI basis. An MSTP-enabled device can have different priorities in different MSTIs.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

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 parameters related to the MST region, including the region name, VLAN-to-MSTI 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 value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

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.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- 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.

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 value of *instance-id* ranges from 0 to 31. The minimum value is 0, representing the CIST.

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:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- 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. 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 the root bridge or a secondary root bridge, you cannot change the priority of the device.

Examples

Specify the current device as the 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 port view, port group view, Layer-2 aggregate port 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 disable the root guard function on the port(s).

By default, the root guard function is disabled.

Note that:

- Configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Enable the root guard function for GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

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

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

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 times the device deletes forwarding address entries within a certain period of time immediately after it receives the first TC-BPDU, in the range of 1 to 255.

Description

Use the **stp tc-protection threshold** command to configure the maximum number of times the device deletes forwarding address entries within 10 seconds immediately after it receives the first TC-BPDU.

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

By default, the device deletes forwarding address entries a maximum of six times within a certain period of time immediately after it receives the first TC-BPDU.

Examples

Set the maximum number of times the device deletes forwarding address entries within a certain period of time immediately 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 *centi-seconds*

undo stp timer forward-delay

View

System view

Default Level

2: System level

Parameters

centi-seconds: Forward delay in centiseconds, ranging form 400 to 3000 in steps 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 set forward delay value; for a secondary 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:

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

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter of the switched network in 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 *centi-seconds*

undo stp timer hello

View

System view

Default Level

2: System level

Parameters

centi-seconds: Hello time (in centiseconds), ranging from 100 to 1000 in steps 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 on the device, while secondary 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:

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

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter of the switched network in 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 *centi-seconds*

undo stp timer max-age

View

System view

Default Level

2: System level

Parameters

centi-seconds: Max age (in centiseconds), ranging from 600 to 4000 in steps 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:

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

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter in 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 *number*

undo stp timer-factor

View

System view

Default Level

2: System level

Parameters

number: Timeout factor, in the range of 1 to 20.

Description

Use the **stp timer-factor** command to configure the timeout time of the device by setting the timeout factor. Timeout time = timeout factor × 3 × hello time.

Use the **undo stp timer-factor** command to restore the default timeout factor.

By default, the timeout factor of the device is set to 3.

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 (by setting the timeout factor to 4 or more). 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 *packet-number*

undo stp transmit-limit

View

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

Default Level

2: System level

Parameters

packet-number: Maximum number of MSTP packets that the port(s) can send within each hello time, namely the maximum transmission rate of the port, in the range of 1 to 255.

Description

Use the **stp transmit-limit** command to set the maximum transmission rate of the port(s).

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.

Note that:

- Configured in port view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate port view, the setting takes effect only on the aggregate port. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- A larger maximum transmission rate value represents more MSTP packets that the port will send within each hello time, but this means that more device resources will be used. An appropriate maximum transmission rate setting can prevent MSTP from using excessive bandwidth resources during network topology changes.

Examples

Set the maximum transmission rate of port GigabitEthernet 2/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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, ranging from 1 to 31.

Description

Use the **vlan-mapping modulo** command to map VLANs in the current MST region to MSTIs according to the specified modulo value.

By default, all VLANs are mapped to the CIST (MSTI 0).

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.

Note

By using the **vlan-mapping modulo** command, you can quickly specify a VLAN for each MSTI. 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**, **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
```

Table of Contents

1 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: Control VLAN ID, in the range 2 to 4093.

Description

Use the **control-vlan** command to specify a control VLAN for an RRPP domain.

Use the **undo control-vlan** command to remove the control VLAN configured for an RRPP domain.

Note that:

- The control VLAN must be a new one.
- You need only configure a control VLAN for the primary ring. However, the control VLAN of a subring is assigned automatically by the system and its VLAN ID is the control VLAN ID of the primary ring plus 1. So, you should select two consecutive new VLANs. Otherwise, the configuration fails.
- Before configuring rings for an RRPP domain, make sure the RRPP domain is configured with a control VLAN.
- Before configuring RRPP rings for an RRPP domain, you can delete or modify the control VLAN configured for the RRPP domain. However, after configuring RRPP rings for an RRPP domain, you cannot delete or modify the control VLAN of the domain.
- Deleting an RRPP domain deletes its control VLAN at the same time.
- You cannot use the **undo vlan all** command to delete a control VLAN.
- Do not enable QinQ or VLAN mapping on the control VLAN. Otherwise, RRPPDUs cannot be forwarded properly.

Related commands: **rrpp domain**, **protected-vlan**.

Examples

Configure the control VLAN of RRPP domain 1 as VLAN 100.

```
<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 information of RRPP configuration.

Examples

Display the brief information of RRPP configuration.

```
<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        GigabitEthernet3/0/1 GigabitEthernet3/0/2  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
 1      0       T       GigabitEthernet3/0/3  GigabitEthernet3/0/4  Yes
 2      1       E       GigabitEthernet3/0/3  GigabitEthernet3/0/5  Yes
                        GigabitEthernet3/0/4
```

Table 1-1 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 and 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 an 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 configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 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 and 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: Ring group ID, in the range 1 to 8.

Description

Use the **display rrpp ring-group** command to display the ring group configuration. If no ring group ID is specified, the configuration of all ring groups is displayed. For an edge node ring group, the subring sending Edge-Hello packets is also displayed.

Related commands: **domain ring**.

Examples

Display the ring group configuration.

```
<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 send Edge-Hello packet

Ring Group 2:
domain 1 ring 4, 6 to 7
domain 2 ring 4, 6 to 7
```

Table 1-2 display rrpp ring-group command output description

Field	Description
Ring Group xx	RRPP ring group ID
domain xx ring xx	Subrings in the ring group
domain xx ring xx send Edge-Hello packet	The subring sending Edge-Hello packets in the ring group

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 RRPP message statistics.

Note that:

- If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device appears. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain appears.
- If some port belongs to more than one ring, its packets are taken statistics based on the rings. You will view the statistics of the port under the current ring.
- When a ring transits from inactive status into active status, its packets will be counted again..

Related commands: **reset rrpp statistics**.

Examples

Display RRPP message statistics of 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  : GigabitEthernet3/0/1
 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: GigabitEthernet3/0/2
 Packet            Link        Common      Complete   Edge  Major Packet
 Direct Hello      Down        Flush FDB   Flush FDB  Hello Fault Total
--------------------------------------------------------------------------
 Send   0           0           0           0         0     0     0
 Rcv    16378       0           0           1         0     0     16379
```

Display RRPP message statistics of RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Active Status : Yes
Primary port  : GigabitEthernet3/0/3
 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: GigabitEthernet3/0/4
 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   : GigabitEthernet3/0/3
 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   : GigabitEthernet3/0/4
 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     : GigabitEthernet3/0/5
 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 1-3 display rrpp statistics command output description

Field	Description
Ring ID	RRPP ring ID
Ring Level	RRPP ring level: 0 for primary ring and 1 for subring
Node Mode	Node mode: master node, transit node, edge node and assistant edge node
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive (An RRPP is active only if the RRPP ring is enabled and the RRPP protocol is globally enabled)
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.
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

Field	Description
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 information about RRPP configuraiton.

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  : GigabitEthernet3/0/1    Port status: UP
```

```
Secondary port: GigabitEthernet3/0/2    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  : GigabitEthernet3/0/4    Port status: UP
Secondary port: GigabitEthernet3/0/5    Port status: BLOCKED

Ring ID       : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : -
Enable Status : No    Active Status: No
Common port   : GigabitEthernet3/0/4    Port status: -
                GigabitEthernet3/0/5    Port status: -
Edge port     : GigabitEthernet3/0/3    Port status: -
```

Table 1-4 display rrpp verbose command output description

Field	Description
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of the RRPP domain, including major control VLAN and sub control VLAN
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 configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 1 representing subring
Node Mode	Node mode: master node, transit node, edge node and 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; and “–” appears in all the other cases.
Enable Status	RRPP ring enable status: Yes indicates enabled and No indicates disabled

Field	Description
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive The current ring is active only when the RRPP protocol and the RRPP ring are enabled simultaneously. Through this field, you can get to know the enable status of the RRPP protocol.
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

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 a ring group.

Use the **undo domain ring** command to remove the specified subring(s) from a ring group. If no subring ID list is specified, all subrings in the ring group are removed in the specified domain.

Note that:

- You can configure ring groups only on edge nodes or assistant-edge nodes.
- 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.
- To assign an activated ring to a ring group, first assign the ring to the assistant-edge node ring group and then to the edge node ring group.
- To remove an activated ring from a ring group, first remove the ring from the edge node ring group and then from the assistant-edge node 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.

Related commands: **rrpp ring-group**, **display rrpp ring-group**.

Examples

Configure subrings for 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. You can use the **display stp region-configuration** command to check the VLANs corresponding to the specified MSTIs.

Use the **undo protected-vlan** command to remove the 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:

- Before configuring rings for an RRPP domain, you must configure protected VLANs for the domain first.
- 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.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- When the VLAN-to-MSTI mappings change, the protected VLANs of an RRPP domain also changes according to the MSTIs configured for the domain.
- All the VLANs permitted to pass through RRPP ports must be configured as protected VLANs of the RRPP domain.
- 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.

Related commands: **rrpp domain**, **control-vlan**, **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 RRPP message statistics.

If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device is cleared. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain is cleared.

Related commands: **display rrpp statistics**.

Examples

Clear the RRPP message 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.

secondary-port: Specifies the port as a secondary port.

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

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 port as an edge port.

Description

Use the **ring** command to configure the node mode of the device and the role of the port accessing the RRPP ring.

Use the **undo ring** command to remove the configuration.

Ports connected to an RRPP ring must conform to the following conditions:

- The link type of these ports must be trunk.
- They must be Layer 2 Ethernet ports, Layer 2 GE ports or Layer 2 aggregate ports.
- They must not be member ports of any aggregation group, service loopback group, or smart link group.
- STP, 802.1x, MAC address authentication and Voice VLAN are all disabled on them.

Note that:

- RRPP ports cannot be configured if the RRPP ring is enabled.
- Make sure the control VLAN exists before configuring the RRPP ring.

- Before configuring rings for an RRPP domain, configure the protected VLANs for the RRPP domain first.
- You must first configure the primary ring and then the subring when configuring an RRPP domain. A ring ID cannot be applied to more than one RRPP ring in the same RRPP domain.
- 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.
- Modifying the node mode, port mode and ring level of an RRPP ring is prohibited after configuration. If needed, you must first delete the existing configuration.
- You must configure the primary ring and then subrings when you configure the edge node and the assistant edge node.
- Moreover, you must remove all subring configurations before deleting the primary ring configuration of the edge node and the assistant edge node. However, the enabled RRPP ring cannot be deleted.

Related command: **control-vlan**, **protected-vlan**, and **ring enable**.

Examples

Specify the device as the master node of primary ring 10 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 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 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 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 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
```

Specify the device as the master node of subring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 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 3/0/1
secondary-port gigabitethernet 3/0/2 level 1
```

Specify the device as the transit node of primary ring 20 in RRPP domain 1, GigabitEthernet 3/0/1 as the primary port and GigabitEthernet 3/0/2 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 3/0/1
secondary-port gigabitethernet 3/0/2 level 1
```

Specify the device as the edge node of primary ring 20 in RRPP domain 1, and GigabitEthernet 3/0/1 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 20 node-mode edge edge-port gigabitethernet 3/0/1
```

Specify the device as the assistant edge node of primary ring 20 in RRPP domain 1, and GigabitEthernet 3/0/1 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 20 node-mode assistant-edge edge-port gigabitethernet 3/0/1
```

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, RRPP protocol and the RRPP ring must be enabled simultaneously.

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  3/0/1
secondary-port gigabitethernet 3/0/2 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 VLAN of it will be deleted at the same time.
- When you delete an RRPP domain, you must ensure it has no RRPP ring.

Related commands: **control-vlan**, **ring**, **ring enable**, **rrpp enable**, **timer**.

Examples

Create RRPP domain 1.

```
<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, RRPP protocol and the RRPP ring must be enabled simultaneously.

Related commands: **ring enable**.

Examples

Enable 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: Ring group ID, in the range 1 to 8.

Description

Use the **rrpp ring-group** command to create an RRPP ring group and enter ring group view.

Use the **undo rrpp ring-group** command to delete an RRPP ring group. After removing a ring group, all subrings in the ring group do not belong to any ring group.

Note that:

- The subrings assigned to the same ring group must have the same edge node. Similarly, they must have the same assistant-edge node. Additionally, these subrings must have the same link in the primary ring.
- As an edge node ring group and an assistant-edge node group are configured on different devices. If the two groups are configured with different subrings, the ring group function fails.
- To remove a ring group, remove the edge node ring group, and then the corresponding assistant-edge node ring group.

- RRPP configured with ring groups cannot interoperate with RRPP that does not support ring group configuration.

Related commands: **domain ring**, **display rrpp ring-group**.

Examples

Create 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 specify the value of the timers of 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
```

Table of Contents

1 Port Mirroring Configuration Commands

Port Mirroring Configuration Commands

display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View

Any view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

all: Specifies all the port mirroring groups.

local: Specifies local port mirroring groups.

remote-destination: Specifies remote destination port mirroring groups.

remote-source: Specifies remote source port mirroring groups.

Description

Use the **display mirroring-group** command to display the information about a port mirroring group or multiple port mirroring groups.

The output information varies with port mirroring group type and is organized by mirroring group numbers.

Examples

Display the information about all the port mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet2/0/1  both
    monitor port: GigabitEthernet2/0/10
mirroring-group 2:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet2/0/3  both
```

```
monitor egress port: GigabitEthernet2/0/11
remote-probe vlan: 200
```

Table 1-1 Description on the fields of the **display mirroring-group** command

Field	Description
mirroring-group	Port mirroring group number
type	Port mirroring group type, which can be local, remote-source, and remote-destination.
status	Status of a port mirroring group. “active” for already effective, and “inactive” for not effective yet.
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 *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View

System view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

all: Removes All the port mirroring groups.

local: Creates/Removes a local port mirroring group.

remote-destination: Creates/Removes a remote destination port mirroring group.

remote-source: Creates/Removes a remote source port mirroring group.

Description

Use the **mirroring-group** command to create a port mirroring group.

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

You need to specify the type of the port mirroring group to be created when creating it.

- Use the keyword **local** to create a local port mirroring group.
- Use the keyword **remote-destination** to create a remote destination port mirroring group.
- Use the keyword **remote-source** to create a remote source port mirroring group.

You need to specify the port mirroring group type or the mirroring group number when removing a port mirroring group:

- Use the *group-id* argument to specify the port mirroring group to be removed.
- Use the **all** keyword to remove all the port mirroring groups.
- Use the **local** keyword to remove all the local port mirroring groups.
- Use the **remote-destination** keyword to remove all the remote destination port mirroring groups.
- Use the **remote-source** keyword to remove all the remote source mirroring groups.

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 *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

View

System view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

mirroring-port-list: List of ports to be added to the port mirroring group. You can specify multiple ports by providing this argument in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where the *interface-type* argument is port type, the *interface-number* argument is the port number, and &<1-8> means that you can provide up to eight port indexes/port index lists for this argument.

both: Specifies to duplicate both inbound and outbound packets.

inbound: Specifies to duplicate inbound packets only.

outbound: Specifies to duplicate outbound packets only.

Description

Use the **mirroring-group mirroring-port** command to configure source ports for a port mirroring group.

Use the **undo mirroring-group mirroring-port** command to remove source ports from a port mirroring group.

Note that:

- The source port cannot be a member port of the current mirroring group.
- A remote destination mirroring group cannot contain source mirroring ports.

Examples

Add ports to port mirroring group 1 as source ports (assuming that port mirroring group 1 already exists).

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port Ethernet 2/0/1 to Ethernet 2/0/5 both
```

Remove source mirroring ports from port mirroring group 1.

```
[Sysname] undo mirroring-group 1 mirroring-port Ethernet 2/0/1 to Ethernet 2/0/3 both
```

mirroring-group monitor-egress

Syntax

- In system view:

mirroring-group *group-id* **monitor-egress** *monitor-egress-port-id*

undo mirroring-group *group-id* **monitor-egress** *monitor-egress-port-id*

- In Ethernet port view:

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

View

System view, Ethernet port view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

monitor-egress-port-id: Index of the port to be configured as the outbound mirroring port. You need to provide this argument in the format of { *interface-type interface-number* }, where *interface-type* is port type and *interface-number* is port number.

Description

Use the **mirroring-group monitor-egress** command to configure a port as the outbound mirroring port of a remote port mirroring group.

Use the **undo mirroring-group monitor-egress** command to remove the outbound mirroring port configured from a remote port 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 Ethernet 2/0/1 as the outbound mirroring port of remote port mirroring group 1 in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress Ethernet 2/0/1
```

Configure port Ethernet 2/0/2 as the outbound mirroring port of remote port mirroring group 2 in Ethernet port view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface Ethernet 2/0/2
[Sysname-Ethernet2/0/2] mirroring-group 2 monitor-egress
```

mirroring-group monitor-port

Syntax

mirroring-group *group-id* **monitor-port** *monitor-port-id*

undo mirroring-group *group-id* **monitor-port** *monitor-port-id*

View

System view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

monitor-port-id: Port index. You need to provide this argument in the form of *interface-type interface-number*, where *interface-type* is the port type and *interface-number* is the port number.

Description

Use the **mirroring-group monitor-port** command to configure the destination port for a port mirroring group.

Use the **undo mirroring-group monitor-port** command to remove the destination port from a port mirroring group.

Note that:

- 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 Ethernet 2/0/1 as the destination port of port mirroring group 1 (a remote destination port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
[Sysname] mirroring-group 1 monitor-port Ethernet 2/0/1
```

mirroring-group remote-probe vlan

Syntax

mirroring-group *group-id* **remote-probe vlan** *rprobe-vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *rprobe-vlan-id*

View

System view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

rprobe-vlan-id: ID of the VLAN to be configured as the remote mirroring VLAN. Note that the VLAN must be an existing static VLAN.

Description

Use the **mirroring-group remote-probe vlan** command to specify a VLAN as the mirroring VLAN for a remote source port mirroring group or a remote destination port mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the remote mirroring VLAN from a remote source mirroring group or a remote 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 mirroring 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** *group-id*] **mirroring-port** { **inbound** | **outbound** | **both** }

undo [**mirroring-group** *group-id*] **mirroring-port** { **inbound** | **outbound** | **both** }

View

Ethernet port view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

both: Duplicates both inbound and outbound packets.

inbound: Duplicates the inbound packets only.

outbound: Duplicates the outbound packets only.

Description

Use the **mirroring-port** command to configure a port as a source mirroring port of a port mirroring group.

Use the **undo mirroring-port** command to remove a source mirroring port from a port mirroring group.

Note that:

- If you do not specify the **mirroring-group** *group-id* keyword-argument combination, these two commands apply to port mirroring group 1.
- The source port cannot be a member port of the current mirroring group.
- A remote destination mirroring group cannot contain source mirroring ports.

Examples

Configure Ethernet 2/0/1 as a source mirroring port of remote source port mirroring group 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] mirroring-group 2 mirroring-port both
```

monitor-port

Syntax

[**mirroring-group** *group-id*] **monitor-port**

undo [**mirroring-group** *group-id*] **monitor-port**

View

Ethernet port view

Default Level

2: System level

Parameters

group-id: Port mirroring group number, in the range of 1 to 4.

Description

Use the **monitor-port** command to configure a port as the destination mirroring port of a port mirroring group.

Use the **undo monitor-port** command to remove the destination mirroring port from a port mirroring group.

If you do not specify the **mirroring-group** *group-id* keyword-argument combination, the **monitor-port** command adds the current port to port mirroring group 1.

Note that:

- If you do not specify the **mirroring-group** *group-id* keyword-argument combination, these two commands apply to port mirroring group 1.
- A remote source mirroring group cannot contain destination mirroring ports.
- Member ports of existing port mirroring groups cannot be destination ports.
- The remote destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- Before adding 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

Add port Ethernet 2/0/1 to port mirroring group 1 (a local port mirroring group) as the destination port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] monitor-port
```

uni mirroring-port

Syntax

uni *uni-number* **mirroring-port** { **both** | **inbound** | **outbound** }

undo uni *uni-number* **mirroring-port**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

both: Mirrors both inbound and outbound packets on the port.

inbound: Mirrors only inbound packets on the port.

outbound: Mirrors only outbound packets on the port.

Description

Use the **uni mirroring-port** command to configure a UNI as the mirroring port.

Use the **undo uni mirroring-port** command to cancel the configuration of a UNI as the mirroring port.

Examples

Mirror the outbound packets on UNI 1.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] uni 1 mirroring-port outbound
```

uni monitor-port

Syntax

uni *uni-number* **monitor-port**

undo uni *uni-number* **monitor-port**

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

Description

Use the **uni monitor-port** command to configure a UNI as the monitor port.

Use the **undo uni monitor-port** command to cancel the configuration of a UNI as the monitor port.

Examples

Mirror the outbound packets on UNI 1 to UNI 2.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] uni 1 mirroring-port outbound
[Sysname-Onu2/0/1:1] uni 2 monitor-port
```

2 Traffic Mirroring Configuration Commands

Note

On the S7900E series switches, traffic mirroring is achieved mainly through QoS policies and remote port mirroring. For QoS policy configuration commands, refer to *QoS Commands* in the *QoS Volume*.

IP Services Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The IP Services Volume is organized as follows:

Features	Description
IP Address	An IP address is a 32-bit address allocated to a network interface on a device that is attached to the Internet. This document introduces the commands for IP address configuration.
ARP	Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address. This document introduces the commands for ARP, Gratuitous ARP, Proxy ARP and Local Proxy ARP, and ARP Attack Defense configuration.
DHCP	DHCP is built on a client-server model, in which the client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client. This document introduces the commands for DHCP server configuration, DHCP relay agent configuration, DHCP Client configuration, and DHCP Snooping configuration.
DNS	Used in the TCP/IP application, Domain Name System (DNS) is a distributed database which provides the translation between domain name and the IP address. This document introduces the commands for DNS Client and DNS Proxy configuration.
IP Performance	In some network environments, you need to adjust the IP parameters to achieve best network performance. This document introduces the commands for Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network, TCP Attributes and ICMP to Send Error Packets configuration.
UDP Helper	UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified server. This document introduces the commands for UDP Helper configuration.
URPF	Unicast Reverse Path Forwarding (URPF) protects a network against source address spoofing attacks. This document introduces the commands for URPF configuration.

Features	Description
IPv6 Basics	Internet protocol version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet protocol version 4 (IPv4). This document introduces the commands for Basic IPv6 functions configuration, IPv6 NDP configuration, PMTU discovery configuration, IPv6 TCP properties configuration, ICMPv6 packet sending configuration,IPv6 DNS Client configuration.
Tunneling	Tunneling is an encapsulation technique, which utilizes one network transport protocol to encapsulate packets of another network transport protocol and transfer them over the network. This document introduces the commands forIPv6 manually tunnel configuration, 6to4 tunnel configuration, and ISATAP tunnel configuration.
sFlow	Based on packet sampling, Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics. This document introduces the commands for sFlow configuration.

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
DHCP packet deal mode:  global
```

Table 1-1 display ip interface command output description

Field	Description
current state	Current physical state of an interface
Line protocol current state	Current state of the network layer protocol
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 an interface
input packets : 0, bytes : 0, multicasts : 0 output packets : 0, bytes : 0, multicasts : 0	Unicast packets, bytes, and multicast packets received on an interface Unicast packets, bytes, and multicast packets sent on an interface
ARP packet input number: 0 Request packet: 0 Reply packet: 0 Unknown packet: 0	Total number of ARP packets received on an interface, including • ARP request packets • ARP reply packets • Unknown packets
TTL invalid packet number	Number of TTL-invalid packets received on an interface

Field	Description
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	Total number of ICMP packets received on an interface, 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
DHCP packet deal mode	DHCP packet processing mode. This field appears on a DHCP-supported device and can be one of the following values: • global: The DHCP server with the global address pool is enabled on the interface. • relay: The DHCP relay agent is enabled on the interface.

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         VLAN2
```

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 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. Currently, up to seven secondary IP addresses are supported on an 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 obtain an IP address through 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
```

Table of Contents

1 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, configuring such a static ARP entry is not allowed; otherwise, the system displays error messages.

Use the **undo arp check enable** command to disable the function. After the ARP entry check is disabled, you can 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

VLAN interface view

Default Level

2: System level

Parameters

number: Maximum number of dynamic ARP entries that an interface can learn, in the range 1 to 8192.

Description

Use the **arp max-learning-num** command to configure the maximum number of dynamic ARP entries that a VLAN interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

Examples

Specify VLAN-interface 40 to learn up to 500 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 500
```

arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

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.

vpn-instance *vpn-instance-name*: Name of a VPN instance, a case-sensitive string of 1 to 31 characters.

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.

- If both the vlan-id and ip-address arguments are specified, the IP address of the VLAN interface corresponding to the vlan-id argument must belong to the same network segment as the IP address specified by the ip-address argument.
- If no VPN instance is specified in the undo arp command, corresponding ARP entries of all VPN instances are removed.

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 GigabitEthernet2/0/10 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 000f-e201-0000 10 gigabitethernet 2/0/10
```

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-id*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [[**verbose**] [**|** { **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-id*: Displays the ARP entries of the specified slot.

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*.

verbose: Displays detailed information about ARP entries.

|: 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 or the **all** keyword 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 verbose
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
Vpn-instance Name
20.1.1.1         000f-e200-0001  N/A      N/A                   N/A   S
test
193.1.1.70       00e0-fe50-6503  100      GE2/0/1               DIS   D
[No Vrf]
192.168.0.115    000d-88f7-9f7d  1        GE2/0/2               DIS   D
[No Vrf]
192.168.0.39     0012-a990-2241  1        GE2/0/3               DIS   D
[No Vrf]
```

Table 1-1 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
Aging	Aging time for a dynamic ARP entry in minutes. “DIS” means the ARP entry is learned from an interface board. (The detailed aging time can be displayed only when you view the dynamic ARP entries of the specified interface board.)
Type	ARP entry type: D for dynamic, S for static, and A for authorized.
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-id*] [**verbose**] [**|** { **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-id*: Displays the ARP entry for the specified slot.

verbose: Displays the detailed information about ARP entries.

|: 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         000f-e200-0001  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)
```

display arp vpn-instance

Syntax

display arp vpn-instance *vpn-instance-name* [**|** { **begin** | **exclude** | **include** } *regular-expression* | **count**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of VPN instance, a case-sensitive string of 1 to 31 characters excluding spaces. With this argument specified, the ARP entries for a specific VPN instance are displayed.

|: 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 that contains 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 character string for matching, consisting of 1 to 256 characters.

count: Displays the number of ARP entries.

Description

Use the **display arp vpn-instance** command to display the ARP entries for a specified VPN instance.

Related commands: **arp static** and **reset arp.**

Examples

Display ARP entries for the VPN instance named test.

```
<Sysname> display arp vpn-instance test
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
20.1.1.1         000f-e200-0001  N/A      N/A                   N/A   S
```

naturemask-arp enable

Syntax

naturemask-arp enable

undo naturemask-arp enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **naturemask-arp enable** command to cancel the restriction that ARP requests must be from the same subnet. In this case, ARP requests from a natural network are supported.

Use the **undo naturemask-arp enable** command to restore the default.

By default, the support for ARP requests from a natural network is disabled.

Examples

Enable the support for ARP requests from a natural network.

```
<Sysname> system-view
[Sysname] naturemask-arp enable
```

reset arp

Syntax

reset arp { **all** | **dynamic** | **slot** *slot-id* | **static** | **interface** *interface-type interface-number* }

View

User view

Default Level

2: System level

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-id*: Clears the ARP entries for the specified slot.

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-id* specified, the command clears only dynamic ARP entries of the interface or the slot.

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.

Examples

Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

2 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 specified VLAN interface.

Description

Use the **display proxy-arp** command to display the proxy ARP status.

Related commands: **proxy-arp enable**.

Examples

Display the status of the proxy ARP status on VLAN-interface 1.

```
<Sysname> display proxy-arp interface vlan-interface 1
Interface Vlan-interface1
 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, Ethernet 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
```

3 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 3-1 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 support for ARP defense against IP packet attacks is enabled.

Examples

Enable ARP defense against IP packet attacks.

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

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 trust

Syntax

arp detection trust

undo arp detection trust

View

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 GigabitEthernet2/0/1 as an ARP trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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, the checking of the MAC addresses and IP addresses of ARP packets 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
```

arp rate-limit

Syntax

arp rate-limit { **disable** | **rate** *pps* **drop** }

undo arp rate-limit

View

Ethernet port view

Default Level

2: System level

Parameters

disable: Disables ARP packet rate limit.

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 is 100 pps.

Examples

Specify the ARP packet rate on GigabitEthernet 2/0/1 as 30 pps, and exceeded packets are discarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] arp rate-limit rate 30 drop
```

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 3-2 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 GigabitEthernet2/0/1.

```
<Sysname> display arp detection statistics interface gigabitethernet2/0/1
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP         Src-MAC    Dst-MAC    Inspect
GE2/0/1(U)                40         0          0          78
```

Table 3-3 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
```

Table of Contents

1 DHCP Server Configuration Commands

Note

- The DHCP server configuration is supported only on VLAN interfaces and loopback interfaces. The subaddress pool configuration is not supported on loopback interfaces.
- DHCP snooping must be disabled on the DHCP server.

DHCP Server Configuration Commands

bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

undo bims-server

View

DHCP address pool view

Default Level

2: System level

Parameters

ip *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range 1 to 65534.

sharekey *key*: Specifies a shared key for the BIMS server, which is a string of 1 to 16 characters.

Description

Use the **bims-server** command to specify the IP address, port number, and shared key of the BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove the specified BIMS server information.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples

Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey aabbcc
```

bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

View

DHCP address pool view

Default Level

2: System level

Parameters

bootfile-name: Boot file name, a string of 1 to 63 characters.

Description

Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.

Use the **undo bootfile-name** command to remove the specified bootfile name.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.

Examples

Specify the bootfile name aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa
```

dhcp enable

Syntax

dhcp enable

undo dhcp enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

Note

You need to enable DHCP before performing DHCP server and relay agent configurations.

Examples

Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp select server global-pool

Syntax

dhcp select server global-pool [**subaddress**]

undo dhcp select server global-pool subaddress

View

Interface view

Default Level

2: System level

Parameters

subaddress: Supports subaddress allocation. That is, the DHCP server and clients are on the same network segment, and the server allocates IP addresses from the address pool containing the network segment of the first subaddress if several subaddresses exist.

Description

Use the **dhcp select server global-pool** command to enable the DHCP server on specified interface(s). After the interface receives a DHCP request, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool subaddress** command to cancel the support for subaddress allocation.

By default, the DHCP server is enabled on an interface.

Examples

Enable the DHCP server on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select server global-pool
```

dhcp server detect

Syntax

dhcp server detect

undo dhcp server detect

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp server detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

Examples

Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

View

System view

Default Level

2: System level

Parameters

low-ip-address: Start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description

Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

Note that:

- When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.
- When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified with the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify the same address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.
- Using the **dhcp server forbidden-ip** command repeatedly can exclude multiple IP address ranges from allocation.

Related commands: **dhcp server ip-pool**, **network**, **static-bind ip-address**.

Examples

Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

View

System view

Default Level

2: System level

Parameters

pool-name: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

Description

Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove the specified DHCP address pool.

By default, no DHCP address pool is created.

Related commands: **dhcp enable**.

Examples

Create the DHCP address pool identified by 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0]
```

dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

View

System view

Default Level

2: System level

Parameters

number: Number of ping packets, in the range of 0 to 10. 0 means no ping operation.

Description

Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

Examples

Specify the maximum number of ping packets as 10.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

View

System view

Default Level

2: System level

Parameters

milliseconds: Response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. 0 means no ping operation.

Description

Use the **dhcp server ping timeout** command to configure response timeout time of the ping packet on the DHCP server.

Use the **undo dhcp server ping timeout** command to restore the default.

The time defaults to 500 ms.

Examples

Specify the response timeout time as 1000 ms.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp server relay information enable** command to enable the DHCP server to handle Option 82.

Use the **undo dhcp server relay information enable** command to configure the DHCP server to ignore Option 82.

By default, the DHCP server handles Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

display dhcp server conflict

Syntax

display dhcp server conflict { **all** | **ip** *ip-address* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays information about all IP address conflicts.

ip-address: Displays conflict information for the IP address.

Description

Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related commands: **reset dhcp server conflict**.

Examples

Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
    Address             Discover time
    4.4.4.1             Apr 25 2007 16:57:20
    4.4.4.2             Apr 25 2007 17:00:10
 --- total 2 entry ---
```

Table 1-1 display dhcp server conflict command output description

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

display dhcp server expired

Syntax

display dhcp server expired { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the lease expiration information of all DHCP address pools.

ip *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

Description

Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Examples

Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
Global pool:
 IP address       Client-identifier/    Lease expiration          Type
                    Hardware address
 4.4.4.6          3030-3066-2e65-3230-  Apr 25 2007 17:10:47     Release
                   302e-3130-3234-2d45-
                   7468-6572-6e65-7430-
                   2f31

 --- total 1 entry ---
```

Table 1-2 display dhcp server expired command output description

Field	Description
Global pool	Information about lease expiration of a DHCP address pool
IP address	Expired IP addresses
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired
Lease expiration	The lease expiration time
Type	Types of lease expirations. Currently, this field is set to Release.

display dhcp server free-ip

Syntax

display dhcp server free-ip

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp server free-ip** command to display information about assignable IP addresses which have never been assigned.

Examples

Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0              to  10.0.0.255
```

display dhcp server forbidden-ip

Syntax

display dhcp server forbidden-ip

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

Examples

Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
IP Range from 1.1.1.1               to  1.1.1.1
IP Range from 2.2.2.2               to  2.2.2.5
```

display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the binding information of all DHCP address pools.

ip *ip-address*: Displays the binding information of a specified IP address.

pool [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

Description

Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use**.

Examples

Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
Global pool:
 IP address    Client-identifier/    Lease expiration        Type
                  Hardware address
 10.1.1.1       4444-4444-4444        NOT Used                  Manual


 --- total 1 entry ---
```

Table 1-3 display dhcp server ip-in-use command output description

Field	Description
Global pool	Binding information of a DHCP address pool
IP address	Bound IP address
Client-identifier/Hardware address	Client's ID or MAC of the binding
Lease expiration	Lease expiration time
Type	Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. • Manual: Static binding • Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client. • Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client.

display dhcp server statistics

Syntax

display dhcp server statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related commands: **reset dhcp server statistics**.

Examples

Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
    Global Pool:
      Pool Number:                    1
      Binding:
        Auto:                         1
        Manual:                       0
        Expire:                       0
    BOOTP Request:                    10
      DHCPDISCOVER:                   5
      DHCPREQUEST:                    3
      DHCPDECLINE:                    0
      DHCPRELEASE:                    2
      DHCPINFORM:                     0
      BOOTPREQUEST:                   0
    BOOTP Reply:                      6
      DHCPOFFER:                      3
      DHCPACK:                        3
      DHCPNAK:                        0
      BOOTPREPLY:                     0
    Bad Messages:                     0
```

Table 1-4 display dhcp server statistics command output description

Field	Description
Global Pool	Statistics of a DHCP address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings
Manual	The number of static bindings
Expire	The number of expired bindings

Field	Description
BOOTP Request	The number of DHCP requests sent from DHCP clients to the DHCP server, including: • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREQUEST
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients, including: • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY
Bad Messages	The number of erroneous messages

display dhcp server tree

Syntax

display dhcp server tree { **all** | **pool** [*pool-name*] }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the tree organization information of all DHCP address pools.

pool [*pool-name*]: Displays the tree organization information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the tree organization information of all address pools will be displayed.

Description

Use the **display dhcp server tree** command to display the tree organization information of DHCP address pool(s).

Examples

Display the tree organization information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:

Pool name: 0
 network 20.1.1.0 mask 255.255.255.0
 Sibling node:1
 option 2 ip-address 1.1.1.1
```

```
 expired 1 0 0

Pool name: 1
 static-bind ip-address 10.10.1.2 mask 255.0.0.0
 static-bind mac-address 00e0-00fc-0001
 PrevSibling node:0
 expired unlimited
```

Table 1-5 display dhcp server tree command output description

Field	Description
Global pool	Information of a address pool
Pool name	Address pool name
network	Network segment for address allocation
static-bind ip-address 10.10.1.2 mask 255.0.0.0 static-bind mac-address 00e0-00fc-0001	The IP address and MAC address of the static binding
Sibling node	The sibling node of the current node, nodes of this kind in the output information include: • Child node: The child node (subnet segment) address pool of the current node • Parent node: The parent node (nature network segment) address pool of the current node • Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher order the sibling node has. • PrevSibling node: The previous sibling node of the current node
option	Self-defined DHCP options
expired	The lease duration, in the format of day, hour, and minute

dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View

DHCP address pool view

Default Level

2: System level

Parameters

ip-address&<1-8>: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to be removed.

Description

Use the **dns-list** command to specify DNS server addresses in a DHCP address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples

Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCP address pool view

Default Level

2: System level

Parameters

domain-name: Domain name suffix for DHCP clients, a string of 1 to 50 characters.

Description

Use the **domain-name** command to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use the **undo domain-name** command to remove the specified domain name suffix.

No domain name suffix is specified by default.

Related commands: **dhcp server ip-pool**.

Examples

Specify a domain name suffix of mydomain.com for the DHCP clients in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
```

```
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View

DHCP address pool view

Default Level

2: System level

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specified the number of hours, in the range of 0 to 23.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59.

unlimited: Specifies the infinite duration, which is actually 136 years.

Description

Use the **expired** command to specify the lease duration in a DHCP address pool.

Use the **undo expired** command to restore the default lease duration in a DHCP address pool.

The lease duration defaults to one day.

Note that if the lease duration you specified is beyond the year 2106, the system regards the lease as expired.

Related commands: **dhcp server ip-pool**.

Examples

Specify the lease duration as one day, two hours and three minutes in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax

gateway-list *ip-address*&<1-8>

undo gateway-list { *ip-address* | **all** }

View

DHCP address pool view

Default Level

2: System level

Parameters

ip-address&<1-8>: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description

Use the **gateway-list** command to specify gateway address(es) in a DHCP address pool.

Use the **undo gateway-list** command to remove specified gateway address(es) specified for the DHCP client from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

Examples

Specify the gateway address 10.110.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View

DHCP address pool view

Default Level

2: System level

Parameters

ip-address&<1-8>: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description

Use the **nbns-list** command to specify WINS server address(es) in a DHCP address pool.

Use the **undo nbns-list** command to remove the specified WINS server address(es).

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **netbios-type**.

Examples

Specify WINS server address 10.12.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View

DHCP address pool view

Default Level

2: System level

Parameters

b-node: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

p-node: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

m-node: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

h-node: Hybrid node, a combination of a p-node first and b-node second. An h-node is a b-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

Description

Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP address pool.

Use the **undo netbios-type** command to remove the specified client NetBIOS node type.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool**, **nbns-list**.

Examples

Specify the NetBIOS node type as b-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network

View

DHCP address pool view

Default Level

2: System level

Parameters

network-address: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

mask-length: Mask length, in the range of 1 to 30.

mask *mask*: Specifies the IP address network mask, in dotted decimal format.

Description

Use the **network** command to specify the IP address range for dynamic allocation in a DHCP address pool.

Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

Note that you can specify only one network segment for each DHCP global address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **dhcp server forbidden-ip**.

Examples

Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View

DHCP address pool view

Default Level

2: System level

Parameters

code: Self-defined option number, in the range of 2 to 254, excluding 12, 50 to 55, 57 to 61, and 82.

ascii *ascii-string*: Specifies an ASCII string with 1 to 63 characters.

hex *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates that you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates that you can specify up to eight IP addresses, separated by spaces.

Description

Use the **option** command to configure a self-defined DHCP option in a DHCP address pool.

Use the **undo option** command to remove a self-defined DHCP option from a DHCP address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples

Configure the hex digits 0x11 and 0x22 for the self-defined DHCP Option 100 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax

reset dhcp server conflict { **all** | **ip** *ip-address* }

View

User view

Default Level

2: System level

Parameters

all: Clears the statistics of all IP address conflicts.

ip *ip-address*: Clears the conflict statistics of a specified IP address.

Description

Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

Related commands: **display dhcp server conflict**.

Examples

Clears the statistics of all IP address conflicts.

```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View

User view

Default Level

2: System level

Parameters

all: Clears the IP address dynamic binding information of all DHCP address pools.

ip *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description

Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related commands: **display dhcp server ip-in-use**

Examples

Clear the binding information of IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics**.

Examples

Clear the statistics of the DHCP server.

```
<Sysname> reset dhcp server statistics
```

static-bind client-identifier

Syntax

static-bind client-identifier *client-identifier*

undo static-bind client-identifier

View

DHCP address pool view

Default Level

2: System level

Parameters

client-identifier: The client ID of a static binding, a string with 4 to 160 characters in the format of H-H-H…, each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, while aabb-c-dddd and aabb-cc-dddd are both invalid.

Description

Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

Note that:

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind ip-address**, **static-bind mac-address**, **display dhcp client verbose**.

Examples

Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View

DHCP address pool view

Default Level

2: System level

Parameters

ip-address: IP address of a static binding. If no mask and mask length is specified, the natural mask is used.

mask-length: Mask length of the IP address, that is, the number of ones in the mask, in the range of 0 to 32.

mask *mask*: Specifies the IP address mask, in dotted decimal format.

Description

Use the **static-bind ip-address** command to specify an IP address in a DHCP address pool for a static binding.

Use the **undo static-bind ip-address** command to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

Note that:

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- If the statically bound IP address is an interface address of the DHCP server, the static binding does not take effect.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind mac-address**.

Examples

Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax

static-bind mac-address *mac-address*

undo static-bind mac-address

View

DHCP address pool view

Default Level

2: System level

Parameters

mac-address: The MAC address of a static binding, in the format of H-H-H.

Description

Use the **static-bind mac-address** command to statically bind a MAC address to an IP address in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the statically bound MAC address.

By default, no MAC address is statically bound.

Note that:

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind ip-address.**

Examples

Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

View

DHCP address pool view

Default Level

2: System level

Parameters

domain-name: TFTP server name, a string of 1 to 63 characters.

Description

Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

Examples

Specify the TFTP server name as aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

View

DHCP address pool view

Default Level

2: System level

Parameters

ip-address: TFTP server IP address.

Description

Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

Examples

Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

View

DHCP address pool view

Default Level

2: System level

Parameters

as-ip *ip-address*: Specifies IP address for the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and "*".

ncp-ip *ip-address*: Specifies IP address for the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

- **disable**: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.
- **enable**: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

Description

Use the **voice-config** command to configure specified Option 184 contents in a DHCP address pool.

Use the **undo voice-config** command to remove specified Option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

Note that specifying the IP address of a network calling processor first is necessary to make other configured parameters take effect.

Examples

Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

2 DHCP Relay Agent Configuration Commands

Note

- The DHCP relay agent configuration is supported only on VLAN interfaces.
- DHCP snooping cannot be configured on the DHCP relay agent.

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.

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** | **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.

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.

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. The specified server group must be an existing group containing at least a DHCP server.

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 an interface on the relay agent can only be correlated to 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.

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.

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-interface2                 2
```

Table 2-1 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     Eth1/1
 10.1.1.5       00e0-0000-0000  Static     Vlan2
---   2 dhcp-security item(s) found   ---
```

Table 2-2 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 2-3 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 2-4 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
```

3 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 switch. Otherwise, DHCP snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.
- You cannot configure an interface of an aggregation group as a DHCP client.

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
 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 3-1 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
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

Field	Description
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
```

4 DHCP Snooping Configuration Commands

Note

- DHCP snooping supports no link aggregation. If an Ethernet port is added into an aggregation group, DHCP snooping configuration on it will not take effect. When the port is removed from the group, DHCP snooping can take effect.
- The DHCP snooping enabled switch 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.
- The DHCP snooping enabled switch cannot be a DHCP server or DHCP relay agent.
- You are not recommended to enable the DHCP client, and DHCP snooping on the same switch. Otherwise, DHCP snooping entries may fail to be generated, or the 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

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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

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 2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information circuit-id string company001
```

dhcp-snooping information enable

Syntax

dhcp-snooping information enable

undo dhcp-snooping information enable

View

Ethernet port 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 gigabitethernet2/0/1
[Sysname-GigabitEthernet2/0/1] 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

Ethernet port 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 gigabitethernet2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information strategy replace
[Sysname-GigabitEthernet2/0/1] 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

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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

Ethernet port 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 gigabitethernet2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet2/0/1] dhcp-snooping information strategy keep
```

dhcp-snooping trust

Syntax

dhcp-snooping trust [**no-user-binding**]

undo dhcp-snooping trust

View

Ethernet port 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.

Related commands: **display dhcp-snooping trust**.

Examples

Specify GigabitEthernet 2/0/1 as a trusted port and enable it to record the IP-to-MAC bindings of clients.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 IP-to-MAC binding corresponding to the specified IP address.

Description

Use the **display dhcp-snooping** command to display the IP-to-MAC bindings recorded by the DHCP snooping device.

Related commands: **dhcp-snooping**.

Note

Using the **display dhcp-snooping** command displays IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages.

Examples

Display all IP-to-MAC bindings recorded by the DHCP snooping device.

```
<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        000f-e200-0006   286        1 GigabitEthernet2/0/1
---   1 dhcp-snooping item(s) found   ---
```

Table 4-1 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 Ethernet ports.

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: GigabitEthernet 2/0/1
    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: GigabitEthernet 2/0//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 board in a specified slot.

Description

Use the **display dhcp-snooping packet statistics** command to display DHCP packet statistics on the DHCP snooping device.

On the S7900E series Ethernet switches, executing the **display dhcp-snooping packet statistics** command without the **slot** keyword only displays DHCP packet statistics on the SRPU.

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
 ========================                  ============
 GigabitEthernet2/0/1                                Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabitEthernet 2/0/1 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 binding information.

ip *ip-address*: Clears the DHCP snooping binding information of the specified IP address.

Description

Use the **reset dhcp-snooping** command to clear DHCP snooping binding information.

For the S7900E series Ethernet switches, DHCP snooping binding information on all slots will be cleared after you execute this command.

Examples

Clear all DHCP binding information.

```
<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 board in a specified slot.

Description

Use the **reset dhcp-snooping packet statistics** command to clear DHCP packet statistics on the DHCP snooping device.

On the S7900E series Ethernet switches, executing the **reset dhcp-snooping packet statistics** command without the **slot** keyword only clears DHCP packet statistics on the SRPU.

Examples

Clear DHCP packet statistics on the DHCP snooping device.

```
<Sysname> reset dhcp-snooping packet statistics
```

Table of Contents

1 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 1-1 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 1-2 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 proxy table

Syntax

display dns proxy table

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dns proxy table** command to display the DNS proxy table.

Examples

Display the DNS proxy table.

```
<Sysname> display dns proxy table
Total entries: 1
Source IP          Source Port  Trans ID     Server IP          Aging
192.168.0.98       1030         24580        192.168.111.244    35
```

Table 1-3 display dns proxy table command output description

Field	Description
Source IP	Source IP address of the DNS request, that is, the IP address of the DNS client.
Source Port	Source port number of the DNS request
Trans ID	Transaction ID of the DNS request
Server IP	IP address of the DNS server
Aging	Aging time of the DNS proxy table entry in seconds

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     172.16.1.1
```

Table 1-4 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 1-5 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
```

Table of Contents

1 IP Performance Configuration Commands

IP Performance Configuration Commands

display fib

Syntax

display fib [**|** { **begin** | **include** | **exclude** } *regular-expression* | **acl** *acl-number* | **ip-prefix** *ip-prefix-name* | **vpn-instance** *vpn-instance-name* [**include** *regular-expression*]]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays FIB entries of the specified VPN instance. The *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

|: 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 a specific FIB entry and all the FIB entries following it. The specific FIB entry is the first entry that matches the specified regular expression.

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.

ip-prefix *ip-prefix-name*: Displays FIB entries matching a specified IP prefix list, a string of 1 to 19 characters.

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.

```
FIB Table:
Total number of Routes : 4

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
```

```
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask   Nexthop      Flag TimeStamp       Interface    Token
10.2.0.0/16        0.0.0.0       U   t[1150900568]   Vlan1        invalid
10.2.1.1/32        127.0.0.1     HU  t[1150900568]   InLoop0      invalid
127.0.0.0/8        127.0.0.1     U   t[1150623094]   InLoop0      invalid
127.0.0.1/32       127.0.0.1     HU  t[1150623094]   InLoop0      invalid
```

Table 1-1 Description on the fields of the **display fib** command

Field	Description
Total number of Routes	Total number of routes in the FIB table
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”—Refused route • “L”—Route generated by ARP or ESIS
TimeStamp	Time stamp
Interface	Forward interface
Token	LSP index number

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
Route entry matched by access-list 2000:
Summary counts: 2

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask   Nexthop      Flag TimeStamp       Interface    Token
10.2.0.0/16        0.0.0.0       U   t[1150900568]   Vlan1        invalid
10.2.1.1/32        127.0.0.1     HU  t[1150900568]   InLoop0      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:Reject   L:Generated by ARP or ESIS

Destination/Mask   Nexthop      Flag TimeStamp       Interface    Token
10.2.1.1/32        127.0.0.1     HU  t[1150900568]   InLoop0      invalid
127.0.0.0/8        127.0.0.1     U   t[1150623094]   InLoop0      invalid
127.0.0.1/32       127.0.0.1     HU  t[1150623094]   InLoop0      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
Route Entry matched by prefix-list abc0:
Summary count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask   Nexthop      Flag TimeStamp       Interface    Token
10.2.0.0/16        0.0.0.0       U   t[1150900568]   Vlan1        invalid
```

display fib ip-address

Syntax

display fib *ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address1, ip-address2: Destination IP address, in dotted decimal notation. *ip-address1* and *ip-address2* together determine an address range for the FIB entries to be displayed.

mask1, mask2: IP address mask.

mask-length1, mask-length2: Length of IP address mask.

longer: Displays FIB entries that match the specified address/mask and have masks longer than or equal to the mask that a user enters. If no masks are specified, FIB entries that match the natural network address and have the masks longer than or equal to the natural mask will be displayed.

Description

Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

Examples

Display the FIB entries that match the natural network of 10.1.0.0 and have the masks longer than or equal to the natural mask.

```
<Sysname> display fib 10.1.0.0 longer
  Route Entry Count: 2
 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS
Destination/Mask   Nexthop      Flag TimeStamp       Interface    Token
10.0.0.0/8     0.0.0.0      U     t[1141140133]   Vlan1        invalid
10.1.1.1/32        127.0.0.1    HU    t[1141140133]   InLoop0      invalid
```

For description about the above output, refer to Table 1-1.

display fib statistics

Syntax

display fib statistics [**vpn-instance**]

View

Any view

Parameters

None

Description

Use the **display fib statistics** command to display statistics about the FIB entries.

Examples

View statistics about the FIB entries.

```
<Sysname> display fib statistics
Route Entry Count          : 2
```

Table 1-2 Description on the fields of the **display fib statistics** command

Field	Description
Route Entry Count	Number of FIB entries

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 a slot.

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 1-3 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

Field	Description
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 slot.

Description

Use the **display ip socket** command to display socket information.

Examples

Display all 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 1-4 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
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Sending buffer size of the socket

Field	Description
rcvbuf	Receiving buffer size of the socket
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 slot.

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 1-5 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 1-6 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
Initiated connections		Number of connections initiated
accepted connections		Number of connections accepted
established connections		Number of connections established

Field	Description
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 with MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted with 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
ca3f8244  0.0.0.0:23             0.0.0.0:0              Listening
ca3f8f04  0.0.0.0:80             0.0.0.0:0              Listening
ca3f79c4  0.0.0.0:7547           0.0.0.0:0              Listening
ca562cc4  192.168.0.74:23        192.168.0.2:1650       Established
```

Table 1-7 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 1-8 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
	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 upper layer due to socket buffer being full
	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*: Number of an ACL from 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.

Use the **undo ip forward-broadcast** command to disable an interface from forwarding directed broadcasts.

By default, an interface is disabled from forwarding directed broadcasts.

Examples

Allow VLAN-interface 2 to forward directed broadcasts permitted by 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

2: System 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 disabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send “reassembly timeout” ICMP packets.

Examples

Enable sending ICMP timeout packets.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

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 slot.

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
```

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, ranging from 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: Length of the TCP finwait timer in seconds, ranging from 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 length 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: Receiving/sending buffer size of TCP connection in KB, ranging from 1 to 32.

Description

Use the **tcp window** command to configure the receiving/sending buffer size of TCP connection.

Use the **undo tcp window** command to restore the default.

The TCP receiving/sending buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Examples

Configure the receiving/sending buffer of TCP connection as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

Table of Contents

1 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
```

Table of Contents

1 URPF Configuration Commands

URPF Configuration Commands

ip urpf strict

Syntax

ip urpf strict

undo ip urpf

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ip urpf strict** command to enable URPF check.

Use the **undo ip urpf** command to disable URPF check.

By default, URPF check is disabled.

Note

After URPF is enabled on an S7900E switch, the routing table capacity on a board may decrease to a half. For details, refer to the section of configuring URPF in the operation manual.

Examples

Enable URPF check.

```
<Sysname> system-view
[Sysname] ip urpf strict
```

Table of Contents

1 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.

Examples

Display IPv6 dynamic domain name information.

```
<Sysname> display dns ipv6 dynamic-host
NoHost             IPv6 Address     TTL
1     aaa              2001::2          6
```

Table 1-1 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 1-2 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

slot-number: Displays the IPv6 forwarding information base (FIB) entries of a slot.

ipv6-address: Displays the IPv6 FIB entries for an IPv6 address.

Description

Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

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- 4/15/2008, Time- 15:17:15
Interface  :    InLoopBack0
```

Table 1-3 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.

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 1-4 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.

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 1-5 display ipv6 interface verbose command output description (on a switch)

Field	Description
Vlan-interface2 current state	Physical state of the interface
Line protocol current state	Link layer protocol state of the interface
IPv6 is enabled	IPv6 packet forwarding state of the interface (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)
ND reachable time	Neighbor reachable time

Field	Description
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
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

Field	Description
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 1-6 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.
Protocol	Link layer protocol state of the interface: • down: Indicates that the network layer protocol state of the VLAN interface is down, generally because no IP address is configured. • up: Indicates that the network 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 slot.

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.

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    GE2/0/1   REACH S    -
```

Table 1-7 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

Field	Description
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 slot.

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 1-8 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:* Number of a slot.

Description

Use the **display ipv6 socket** command to display socket information.

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 1-9 display ipv6 socket command output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task 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
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 the slot.

Description

Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets.

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 1-10 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 sent 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
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.

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 1-11 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

Field	Description
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
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.

Examples

Display the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB       Local Address       Foreign Address      State
045d8074     ::->21                ::->0              Listening
```

Table 1-12 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
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.

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 1-13 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::1/64.

```
<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.

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-address*|*prefix-length* **eui-64**

undo ipv6 address *ipv6-address*|*prefix-length* **eui-64**

View

Interface view

Default Level

2: System level

Parameters

ipv6-address|*prefix-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.

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.

```
<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.

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.

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.

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.

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.

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.

Examples

Configure a static neighbor entry for Layer 2 port GigabitEthernet 2/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 gigabitethernet 2/0/1
```

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 of 1 to 2048.

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 an interface is 2048.

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, in the range of 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.

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 slot.

static: Clears static neighbor information on all interfaces.

Description

Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

Examples

Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

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 the slot.

Description

Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets 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.

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.

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
```

Table of Contents

1 Tunneling Configuration Commands

Note

The tunnel interface number is in the A/B/C format, where A, B, and C represent the slot number of a card, the slot number of a sub-card, and the tunnel interface number, respectively. The value ranges of A and B vary with devices, and that of C is from 0 to 1023.

Tunnel Configuration Commands

destination

Syntax

destination *ip-address*

undo destination

View

Tunnel interface view

Default Level

2: System level

Parameters

ip-address: Tunnel destination IPv4 address.

Description

Use the command **destination** to specify the destination address for the tunnel interface.

Use the **undo destination** command to remove the configured tunnel destination address.

By default, no tunnel destination address is configured.

Note that:

- The tunnel destination address is the address of the peer interface receiving packets and should be configured as the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.

Related commands: **interface tunnel**, **source**.

Examples

Set the interface VLAN-interface 100 (193.101.1.1) of Sysname 1 and the interface VLAN-interface 100 (192.100.1.1) of Sysname 2 as the source and destination interfaces of a tunnel between the two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface tunnel 2/0/0
[Sysname1-Tunnel2/0/0] source 193.101.1.1
[Sysname1-Tunnel2/0/0] destination 192.100.1.1
<Sysname2> system-view
[Sysname2] interface tunnel 2/0/1
[Sysname2-Tunnel2/0/1] source 192.100.1.1
[Sysname2-Tunnel2/0/1] destination 193.101.1.1
```

display interface tunnel

Syntax

display interface tunnel [*number*]

View

Any view

Default Level

1: Monitor level

Parameters

number: Tunnel interface number. If the *number* argument is not specified, the information of all tunnel interfaces will be displayed.

Description

Use the **display interface tunnel** command to display related information of a specified tunnel interface, such as source address, destination address, and encapsulation mode.

Related commands: **interface tunnel**, **source**, **destination**, **tunnel-protocol**.

Examples

Display the information of the interface tunnel 2/0/0.

```
<Sysname> display interface tunnel 2/0/0
Tunnel2/0/0 current state: UP
Line protocol current state: UP
Description: Tunnel2/0/0 Interface
The Maximum Transmit Unit is 1476
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 192.13.2.1, destination 192.13.2.2
Tunnel protocol/transport IPv6/IP
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
```

```
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    361 packets input,  9953388 bytes
    0 input error
    361 packets output,  30324 bytes
    0 output error
```

Table 1-1 display interface tunnel command output description

Field	Description
Tunnel2/0/0 current state: UP	The physical-layer connectivity of the tunnel interface is established.
Line protocol current state: UP	The link-layer connectivity of the tunnel interface is established.
Description	Descriptive information of the tunnel interface
Tunnel2/0/0 Interface	Tunnel interface number
Maximum Transmit Unit	Maximum transmission unit (MTU) in the tunnel
Encapsulation is TUNNEL	The encapsulation protocol is tunnel.
service-loopback-group ID	Service loopback group referenced by the tunnel.
Tunnel source	Tunnel source address
destination	Tunnel destination address
Tunnel protocol/transport	Tunnel protocol and transport protocol.
Output queue : (Urgent queuing : Size/Length/Discards)	Packet statistics of the urgent queue
Output queue : (Protocol queuing : Size/Length/Discards)	Packet statistics of the protocol queue
Output queue : (FIFO queuing : Size/Length/Discards)	Packet statistics of the FIFO queue
Last 300 seconds input	Number of bytes and packets input per second in the last five minutes.
Last 300 seconds output	Number of bytes and packets output per second in the last five minutes.
packets input	Total number of input packets.
input error	Number of error packets among all input packets.
packets output	Total number of output packets.
output error	Number of error packets in all output packets

display ipv6 interface tunnel

Syntax

display ipv6 interface tunnel [*number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

number: Tunnel interface number.

verbose: Displays the detailed configuration and IPv6 packet statistics of the specified tunnel interface.

Description

Use the **display ipv6 interface tunnel** command to display the configuration and IPv6 packet statistics of a tunnel interface or all tunnel interfaces.

Note that:

- If no tunnel interface is specified, information about all tunnel interfaces is displayed.
- If the **verbose** keyword is not specified, summary tunnel interface information is displayed.

Examples

Display the detailed information of interface tunnel 2/0/0.

```
<Sysname> display ipv6 interface tunnel 2/0/0 verbose
Tunnel2/0/0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::202:201
  Global unicast address(es):
    3000::1, subnet is 3000::/64
  Joined group address(es):
    FF02::1:FF02:201
    FF02::1:FF00:1
    FF02::1:FF00:0
    FF02::2
    FF02::1
  MTU is 1480 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   45
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
```

```
OutFragFails:                 0
InUnknownProtos:              0
InDelivers:                   45
OutRequests:                  45
OutForwDatagrams:             0
InNoRoutes:                   0
InTooBigErrors:               0
OutFragOKs:                   0
OutFragCreates:               0
InMcastPkts:                  0
InMcastNotMembers:            0
OutMcastPkts:                 0
InAddrErrors:                 0
InDiscards:                   0
OutDiscards:                  0
```

Table 1-2 display interface tunnel command output description

Field	Description
Tunnel2/0/0 current state	The physical-layer state of the tunnel interface
Line protocol current state	The link-layer protocol state of the tunnel interface
IPv6 is enabled	IPv6 forwarding state of the tunnel interface (IPv6 is enabled on the tunnel interface in this example)
link-local address	Link-local address of the tunnel interface
Global unicast address(es)	Aggregatable global unicast address of the tunnel interface.
Joined group address(es)	Multicast address of the tunnel interface.
MTU is 1500 bytes	Size of the MTU in the tunnel.
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor discovery request message.
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire IPv6 addresses.
InReceives	All IPv6 packets received on the tunnel interface, including error packets.
InTooShorts	IPv6 packets that are too short in length received on the tunnel interface, such as a packet with a length less than 40 bytes.
InTruncatedPkts	IPv6 packets received on the tunnel interface, with a length less than that specified in the packet header.
InHopLimitExceeds	IPv6 packets having exceeded the hop limit received on the tunnel interface
InBadHeaders	IPv6 packets with wrong basic headers received on the tunnel interface
InBadOptions	IPv6 packets with wrong extension headers received on the tunnel interface
ReasmReqds	IPv6 fragments received on the tunnel interface

Field	Description
ReasmOKs	Number of IPv6 datagrams reassembled on the tunnel interface.
InFragDrops	Wrong IPv6 fragments discarded on the tunnel interface
InFragTimeouts	IPv6 fragments discarded on the interface because they had stayed in the cache longer than the specified time.
OutFragFails	IPv6 Packets that failed to be fragmented on the outbound tunnel interface
InUnknownProtos	IPv6 packets received on the tunnel interface, with an unknown or unsupported protocol type.
InDelivers	IPv6 packets delivered to the upper-layer IPv6 protocols (such as ICMPv6, TCP, or UDP) from the tunnel interface
OutRequests	Local IPv6 packets from the upper-layer IPv6 protocols
OutForwDatagrams	IPv6 packets forwarded by the outbound tunnel interface
InNoRoutes	IPv6 packets discarded on the interface because no matching route is found
InTooBigErrors	IPv6 packets discarded while being forwarded on the interface due to exceeding MTU values
OutFragOKs	Packets that are successfully fragmented on the outbound interface
OutFragCreates	Fragments on the outbound interface
InMcastPkts	IPv6 multicast packets received on the interface
InMcastNotMembers	IPv6 multicast packets discarded on the interface because the interface does not belong to the corresponding multicast groups
OutMcastPkts	IPv6 multicast packets sent on the interface
InAddrErrors	IPv6 packets discarded on the interface due to illegal destination addresses
InDiscards	IPv6 packets received but then discarded on the interface due to resource problems rather than packet content errors
OutDiscards	IPv6 packets sent on the interface but then discarded due to resource problems rather than packet content errors

Display the summary IPv6 information of the interface tunnel 2/0/0.

```
<Sysname> display ipv6 interface tunnel 2/0/0
*down: administratively down
(s): spoofing
Interface                              Physical   Protocol   IPv6 Address
Tunnel2/0/0                               up         up       3000::1
```

Table 1-3 display ipv6 interface tunnel command output description

Field	Description
*down	The tunnel interface is in administrative down state, meaning the interface is shut down using the **shutdown** command.
(s)	Spoofing feature of the tunnel interface. That is, although the link-layer protocol state of the interface is up, no such link exists, or the link is not a permanent one and can only be established as needed.
Interface	Name of the tunnel interface
Physical	Physical state of the tunnel interface
Protocol	Link-layer protocol state of the tunnel interface
IPv6 Address	IPv6 address of the tunnel interface. Only the first configured IPv6 address is displayed

interface tunnel

Syntax

interface tunnel *number*

undo interface tunnel *number*

View

System view

Default Level

2: System level

Parameters

number: Tunnel interface number. The tunnel interface number is in the A/B/C format, where A, B, and C represent the slot number of a card, the slot number of a sub-card, and the tunnel interface number, respectively. The value ranges of A and B vary with devices, and that of C is from 0 to 1023.

Description

Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove the specified tunnel interface.

By default, there is no tunnel interface on the device.

- Executing the **interface tunnel** command enters interface view of a specified tunnel. If no tunnel interface is created, executing this command first creates a tunnel and then enters the tunnel interface view.
- A tunnel interface number has only local significance, and therefore, the same interface number or different interface numbers can be set at both ends of a tunnel.

Related commands: **display interface tunnel**, **source**, **destination**, **tunnel-protocol**.

Examples

Create the interface tunnel 2/0/3.

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

```
[Sysname] interface tunnel 2/0/3
[Sysname-Tunnel2/0/3]
```

service-loopback-group

Syntax

service-loopback-group *number*

undo service-loopback-group

View

Tunnel interface view

Default Level

2: System level

Parameters

number: Service loopback group ID, in the range of 1 to 1024.

Description

Use the **service-loopback-group** command to reference a service loopback group on the tunnel interface.

Use the **undo service-loopback-group** command to remove the referenced service loopback group from the tunnel interface.

By default, no service loopback group is referenced on a tunnel interface.

The service loopback group to be referenced must have been configured and have the service type set to tunnel in system view.

One tunnel interface can reference only one service loopback group.

Related commands: **service-loopback group** in *Service Loopback Group Commands* in the *Access Volume*.

Examples

Create service loopback group 1 of tunnel type.

```
<Sysname> system-view
[Sysname] service-loopback group 1 type tunnel
```

Add a Layer 2 GigabitEthernet interface to service loopback group 1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp disable
[Sysname-GigabitEthernet1/0/1] port service-loopback group 1
[Sysname-GigabitEthernet1/0/1] quit
```

Reference service loopback group 1 on interface tunnel 2.

```
[Sysname] interface tunnel 2/0/2
[Sysname-Tunnel2/0/2] service-loopback-group 1
```

source

Syntax

source { *ip-address* | *interface-type interface-number* }

undo source

View

Tunnel interface view

Default Level

2: System level

Parameters

ip-address: Tunnel source IPv4 address.

interface-type interface-number: Specifies an interface. The interface types include vlan-interface, tunnel, and loopback.

Description

Use the **source** command to specify the source address or interface of the tunnel interface.

Use the **undo source** command to remove the configured source address or interface of the tunnel interface.

By default, no source address or interface is specified for the tunnel interface.

Note that:

- The tunnel source address is the address of the interface sending packets and should be configured as the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related commands: **interface tunnel**, **destination**.

Examples

Set the tunnel source address to 192.100.1.1 (or the interface VLAN-interface 100) on the interface Tunnel 2/0/5.

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/5
[Sysname-Tunnel2/0/5] source 192.100.1.1
```

Or

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/5
[Sysname-Tunnel2/0/5] source vlan-interface 100
```

tunnel-protocol

Syntax

tunnel-protocol ipv6-ipv4 [**6to4** | **isatap**]

undo tunnel-protocol

View

Tunnel interface view

Default Level

2: System level

Parameters

ipv6-ipv4: Sets the tunnel to an IPv6 manual tunnel.

ipv6-ipv4 6to4: Sets the tunnel to IPv6 over IPv4 6to4 tunnel.

ipv6-ipv4 isatap: Sets the tunnel to an IPv6 over IPv4 ISATAP tunnel.

Description

Use the **tunnel-protocol** command to configure the tunnel mode.

Use the **undo tunnel-protocol** to restore the default tunnel mode.

By default, the tunnel is a IPv6 manual tunnel.

Note that:

- A proper tunnel mode can be selected for packet encapsulation according to the network topology and application. The same tunnel mode must be configured at both ends of the tunnel. Otherwise, packet delivery will fail.
- Only one automatic tunnel can be configured at the same tunnel source.

Examples

Specify the tunnel mode as IPv6 over IPv4 6to4 tunnel interface.

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/2
[Sysname-Tunnel2/0/2] tunnel-protocol ipv6-ipv4 6to4
```

Table of Contents

1 sFlow Configuration Commands

sFlow Configuration Commands

display sflow

Syntax

display sflow [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the sFlow configuration information on a slot.

Description

Use the **display sflow** command to display the sFlow configuration information.

Examples

Display the sFlow configuration information of Slot 2.

```
<Sysname> display sflow slot 2
 sFlow Version: 5
 sFlow Global Information:
    Agent            IP:1.1.1.1
    Collector        IP:2.2.2.2          Port:6343
                       IP:3.3.3.3          Port:6343
    Interval(s): 20
 sFlow Port Information:
    Interface        Direction           Rate      Mode           Status
    GE2/0/1          In/Out               200000    Random          Active
    GE2/0/20         In                     200000    Random          Active
```

Table 1-1 Description on the fields of the **display sflow** command

Field	Description
sFlow Version: 5	The sFlow version is 5
sFlow Global Information	sFlow global information
Agent	IP address of the sFlow agent
Collector	IP address and port number of the sFlow collector

Field	Description
Interval(s)	Counter sampling interval
sFlow Port Information	Information of the ports enabled with sFlow
Interface	sFlow enabled interface
Direction	Packet sampling direction: • In/Out: Samples both inbound and outbound packets. • In: Samples inbound packets. • Out: Samples outbound packets.
Rate	Packet sampling rate
Mode	Packet sampling mode. Random indicates sampling 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 when you execute the **undo sflow agent ip** command.

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 the specified IP address.

By default, no sFlow collector IP address 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 IP address is specified.
- If only one sFlow collector IP address is specified, sFlow does not work after you execute the **undo sflow collector ip** command.

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

Interface 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.

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 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 configure the counter sampling interval.

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

Interface view

Default Level

2: System level

Parameters

determine: Indicates to sample a fixed number of packets.

random: Indicates to 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 S7900E series Ethernet switches.

Examples

Specify the sFlow sampling mode as **random** on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] sflow enable inbound
[Sysname-GigabitEthernet2/0/1] sflow sampling-mode random
```

sflow sampling-rate

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

View

Interface view

Default Level

2: System level

Parameters

rate: Packet sampling rate, in the range of 1000 to 500000.

Description

Use the **sflow sampling-rate** command to configure the packet sampling rate.

Use the **undo sflow sampling-rate** command to restore the default.

By default, the packet sampling rate is 200000, that is, one out of every 200000 packets is sampled.

Note that this command should be used after sFlow is enabled on the current port.

Examples

Configure the packet sampling rate as 100000 on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] sflow enable inbound
[Sysname-GigabitEthernet2/0/1] sflow sampling-rate 100000
```

IP Routing Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The IP Routing Volume is organized as follows:

Features	Description
IP Routing Table Display	This document introduces the Display commands for IP Routing Table.
Static Routing	This document introduces the commands for Static Routing.
RIP	Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks. This document introduces the commands for RIP configuration.
OSPF	Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF. This document introduces the commands for OSPF configuration.
IS-IS	Intermediate System-to-Intermediate System (IS-IS) is a link state protocol, which uses the shortest path first (SPF) algorithm. This document introduces the commands for IS-IS configuration.
BGP	Border gateway protocol (BGP) is an inter-autonomous system (inter-AS) dynamic route discovery protocol. This document introduces the commands for BGP configuration.
IPv6 Static Routing	Similar to IPv4 static routes, IPv6 static routes work well in simple IPv6 network environments. This document introduces the commands for IPv6 Static Routing configuration.
IPv6 RIPng	RIP next generation (RIPng) is an extension of RIP-2 for IPv4. RIPng for IPv6 is IPv6 RIPng. This document introduces the commands for RIPng configuration.
IPv6 OSPFv3	OSPFv3 is OSPF version 3 for short, supporting IPv6 and compliant with RFC2740 (OSPF for IPv6). This document introduces the commands for OSPFv3 configuration.
IPv6 IS-IS	IS-IS with IPv6 support is called IPv6 IS-IS dynamic routing protocol. This document introduces the commands for IPv6 IS-IS configuration.
IPv6 BGP	To support multiple network layer protocols, IETF extended BGP-4 by introducing IPv6 BGP. This document introduces the commands for IPv6 BGP configuration.

Features	Description
Route Policy	Routing policy is used on the router for route inspection, filtering, attributes modifying when routes are received, advertised, or redistributed. This document introduces the commands for Routing Policy configuration.

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.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

IP Routing Table Commands

display ip routing-table

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose** | | { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays routing table information for a VPN instance. The *vpn-instance-name* argument represents the instance name and is a string of 1 to 31 case-sensitive characters.

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: 00h00m30s
        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: 00h00m30s
        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: 00h00m36s
        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: 00h00m36s
        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
RelyNextHop	The next hop address obtained through routing recursion
Neighbour	Neighboring address determined by Routing Protocol
Tunnel ID	Tunnel ID

Field	Description	
Label	Label	
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. Holddown is a route advertisement policy used in some distance vector (D-V) routing protocols, such as RIP, to avoid the propagation of some incorrect routes. It distributes a Holddown route during a period regardless of whether a new route to the same destination is found. For details, refer to corresponding routing protocols.
	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
3.3.3.0/24          Direct 0    0           3.3.3.1       Vlan3
3.3.3.1/32          Direct 0    0           127.0.0.1     InLoop0
4.4.4.0/24          Direct 0    0           4.4.4.1       Vlan4
4.4.4.1/32          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: Vlan2
  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: InLoop0
  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 **bgp**, **direct**, **isis**, **ospf**, **rip**, **static**, or **guard**.

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 [**vpn-instance** *vpn-instance-name*] **statistics**

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays routing table statistics for a VPN instance. The VPN instance name is a string of 1 to 31 case-sensitive characters.

Description

Use the **display ip routing-table statistics** command to display the route statistics of the public network routing table or the VPN 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
RIP         0            0            0            0             0
OSPF        0            0            0            0             0
IS-IS       0            0            0            0             0
BGP         0            0            0            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 ip relay-route

Syntax

display ip relay-route [**vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays the recursive route information of the VPN instance. *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Description

Use the **display ip relay-route** command to display the information of recursive routes.

When executed with no argument, this command displays the recursive route information of the public network routing table.

Examples

Display recursive route information.

```
<Sysname> display ip relay-route
 Total Number of Relay-route is: 1.
 Dest/Mask: 40.40.40.0/255.255.255.0
Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 1-4 display ip relay-route command output description

Field	Description
Total Number of Relay-route	Total number of recursive routes
Dest/Mask	Destination address/mask of the recursive route
Related instance id(s)	The number in the parentheses after each instance ID indicates the number of routes that have used the recursive route in the routing table corresponding to the instance ID.

display ip relay-tunnel

Syntax

display ip relay-tunnel

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ip relay-tunnel** command to display recursive tunnel information.

Examples

Display recursive tunnel information.

```
<Sysname> display ip relay-tunnel
 Total Number of Relay-tunnel is: 1.
 Dest/Mask: 40.40.40.40/255.255.255.255
Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 1-5 display ip relay-tunnel command output description

Field	Description
Total Number of Relay-tunnel	Total number of recursive tunnels
Dest/Mask	Destination address/mask of the recursive tunnel
Related instance id(s)	The number in the parentheses after each instance ID indicates the number of routes that have used the recursive tunnel in the routing table corresponding to the instance ID.

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 1-6 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 1-6 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 1-6 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 1-6 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 1-6 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 **bgp4+**, **direct**, **isisv6**, **ospfv3**, **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 1-6 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
RIPng          0           0           0           0           0
OSPFv3         0           0           0           0           0
IS-ISv6        0           0           0           0           0
BGP4+          0           0           0           0           0
Total          4           1           4           0           0
```

Table 1-7 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 1-8 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
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

display ipv6 relay-route

Syntax

display ipv6 relay-route

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 relay-route** command to display IPv6 recursive route information.

Examples

Display IPv6 recursive route information.

```
<Sysname> display ipv6 relay-route
 Total Number of relay-route is: 1
 Dest/Mask: 192::1/64
      Related instance id(always 0): 0(1)
```

Table 1-9 display ipv6 relay-route command output description

Field	Description
Total Number of Relay-route	Total number of recursive routes
Dest/Mask	Destination address/mask of the recursive route
Related instance id(always 0)	IPv6 supports public networks only. Therefore, the instance ID can be 0 only. The number in the parentheses after the instance ID indicates the number of routes that have used the recursive route in the routing table.

display ipv6 relay-tunnel

Syntax

display ipv6 relay-tunnel

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 relay-tunnel** command to display IPv6 recursive tunnel information.

Examples

Display IPv6 recursive tunnel information.

```
<Sysname> display ipv6 relay-tunnel
 Total Number of relay-tunnel is: 1.
 Dest/Mask: 192::0/64
      Related instance id(always 0): 0(1)
```

Table 1-10 display ipv6 relay-tunnel command output description

Field	Description
Total Number of Relay-tunnel	Total number of recursive tunnels
Dest/Mask	Destination address/mask of the recursive tunnel
Related instance id(always 0)	IPv6 supports public networks only. Therefore, the instance ID can be 0 only. The number in the parentheses after the instance ID indicates the number of routes that have used the recursive route in the routing table.

display router id

Syntax

display router id

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display router id** command to display the router ID.

Examples

Display the router ID.

```
<Sysname> display router id
         Configured router ID is 1.1.1.1
```

router id

Syntax

router id *router-id*

undo router id

View

System view

Default Level

2: System level

Parameters

router-id: Router ID, expressed as an IPv4 address.

Description

Use the **router id** command to configure a router ID.

Use the **undo router id** command to remove the router ID.

By default, no router ID is configured.

Some routing protocols use a router ID to identify a routing device. A route ID is selected in the following sequence:

- Select the router ID configured with the **router id** command;
- Select the highest IP address among loopback interfaces as the router ID:
- If no loopback interface IP address is available, the highest IP address among physical interfaces is selected as the router ID (regardless of the interface state).
- If the interface whose IP address is the router ID is removed or modified, a new router ID is selected. Other events, (the interface goes down; after a physical interface's IP address is selected as the router ID, an IP address is configured for a loopback interface; a higher interface IP address is configured) will not trigger a router ID re-selection.

A VPN instance selects a router ID among interfaces belonging to it according to the preceding procedure.

When a master/backup switchover occurs, the backup device selects a router ID according to the preceding procedure.

After a router ID is changed, you need to use the **reset** command to make it effective.

Examples

Configure a router ID.

```
<Sysname> system-view
[Sysname] router id 1.1.1.1
```

reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { **all** | *protocol* }

View

User view

Default Level

2: System level

Parameters

vpn-instance-name: VPN instance name, a string of 1 to 31 case-sensitive characters.

all: Clears statistics for all routing protocols.

protocol: Clears statistics for the routing protocol, which can be **bgp**, **direct**, **is-is**, **ospf**, **rip**, or **static**.

Description

Use the **reset ip routing-table statistics protocol** command to clear routing statistics for the routing table or VPN routing table.

Examples

Clear routing statistics for the VPN instance **Sysname1**.

```
<Sysname> reset ip routing-table statistics protocol vpn-instance Sysname1 all
```

reset ipv6 routing-table statistics

Syntax

reset ipv6 routing-table statistics protocol { **all** | *protocol* }

View

User view

Default Level

2: System level

Parameters

all: Clears statistics for all routing protocols.

protocol: Clears statistics for the routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

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
```

Table of Contents

1 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 [**vpn-instance** *vpn-instance-name*] **static-routes all**

View

System view

Default Level

2: System level

Parameters

vpn-instance-name: Name of a VPN instance, a string of 1 to 31 case-sensitive characters.

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: **display ip routing-table**, **ip route-static**.

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* | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**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*] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference-value*]

ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } { *next-hop-address* [**track** *track-entry-number*] [**public**] | *interface-type interface-number next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } [*next-hop-address* [**public**] | *interface-type interface-number* [*next-hop-address*] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference-value*]

View

System view

Default Level

2: System level

Parameters

vpn-instance *s-vpn-instance-name*&<1-6>: Specifies the VPN instance name, which is a string of 1 to 31 case-sensitive characters. &<1-6> indicates the argument before it can be entered up to 6 times. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

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.

vpn-instance *d-vpn-instance-name*: Name of the destination VPN instance, case-sensitive. If a destination VPN instance name is specified, the router will search the output interface in the destination VPN instance based on the configured *next-hop-address*.

next-hop-address **public**: Indicates that the specified *next-hop-address* is a public network address, rather than a VPN instance address.

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.

Related commands: **display ip routing-table**, **ip route-static default-preference**.

Note

- The static route does not take effect if you specify its next hop address first and then configure the address as the IP address of a local interface.
- The next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect.
- For a NULL0 interface, if the output interface has already been configured, there is no need to configure the next hop address.
- 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 the track module uses NQA to detect the reachability of the private network static route's nexthop, the VPN instance number of the static route's nexthop must be identical to that configured in the NQA test group.
- 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
```

Configure a static route for a VPN instance named **vpn1**: the destination address is 1.1.1.1/16 and the next hop address is 1.1.1.2, which is the address of this VPN instance.

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

```
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 16 vpn-instance vpn1 1.1.1.2
```

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: **display ip routing-table**, **ip route-static**.

Examples

Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

Table of Contents

1 RIP Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

RIP Configuration Commands

checkzero

Syntax

checkzero

undo checkzero

View

RIP view

Default Level

2: System level

Parameters

None

Description

Use the **checkzero** command to enable the zero field check on RIPv1 messages.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

After the zero field check is enabled, the router discards RIPv1 messages in which zero fields are non-zero. If all messages are trusty, you can disable this feature to reduce the processing time of the CPU.

Examples

Disable the zero field check on RIPv1 messages for RIP process 100.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] undo checkzero
```

default cost (RIP view)

Syntax

default cost *value*

undo default cost

View

RIP view

Default Level

2: System level

Parameters

value: Default metric of redistributed routes, in the range of 0 to 16.

Description

Use the **default cost** command to configure the default metric for redistributed routes.

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

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related command: **import-route**.

Examples

Set the default metric for redistributed routes to 3.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default cost 3
```

default-route

Syntax

default-route { **only** | **originate** } [**cost** *cost*]

undo default-route

View

RIP view

Default Level

2: System level

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost: Cost of the default route, in the range of 1 to 15.

Description

Use the **default-route originate cost** command to configure all the interfaces under the RIP process to advertise a default route with the specified metric to RIP neighbors.

Use the **undo default-route originate** command to disable all the interfaces under the RIP process from sending a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Related commands: **rip default-route**.

Examples

Configure all the interfaces under RIP process 1 to send only a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route only cost 2
```

display rip

Syntax

display rip [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 characters.

Description

Use the **display rip** command to display the current status and configuration information of the specified RIP process.

- If *process-id* is not specified, information about all configured RIP processes is displayed.
- If *vpn-instance-name* is specified, the RIP configuration of the specified VPN instance is displayed.

Examples

Display the current status and configuration information of all configured RIP processes.

```
<Sysname> display rip
  Public VPN-instance name :

    RIP process : 1
       RIP version : 1
       Preference : 100
```

```
Checkzero : Enabled
Default-cost : 0
Summary : Enabled
Hostroutes : Enabled
Maximum number of balanced paths : 8
Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
Suppress time :  120 sec(s)  Garbage-collect time :  120 sec(s)
update output delay :   20(ms)  output count :    3
TRIP retransmit time :    5 sec(s)
TRIP response packets retransmit count :   36
Silent interfaces : None
Default routes : Only  Default route cost : 3
Verify-source : Enabled
Networks :
    192.168.1.0
Configured peers : None
Triggered updates sent : 0
Number of routes changes : 0
Number of replies to queries : 0
```

Table 1-1 display rip command output description

Field	Description
Public VPN-instance name (or Private VPN-instance name)	The RIP process runs under a public VPN instance/The RIP process runs under a private VPN instance
RIP process	RIP process ID
RIP version	RIP version 1 or 2
Preference	RIP route priority
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages.
Default-cost	Default cost of the redistributed routes
Summary	Indicates whether route summarization is enabled
Hostroutes	Indicates whether to receive host routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIP update interval
Timeout time	RIP timeout time
Suppress time	RIP suppress interval
update output delay	RIP packet sending interval
output count	Maximum number of RIP packets sent at each interval
Garbage-collect time	RIP garbage collection interval
TRIP retransmit time	TRIP retransmit interval for sending update requests and responses.
TRIP response packets retransmit count	Maximum retransmit times for update requests and responses

Field	Description
Silent interfaces	Number of silent interfaces, which do not periodically send updates
Default routes	Indicates whether a default route is sent to RIP neighbors • **only** means only a default route is advertised. • **originate** means a default route is advertised along with other routes. • **disable** means no default route is advertised.
Default route cost	Cost of the default route
Verify-source	Indicates whether the source IP address is checked on the received RIP routing updates
Networks	Networks enabled with RIP
Configured peers	Configured neighbors
Triggered updates sent	Number of sent triggered updates
Number of routes changes	Number of changed routes in the database
Number of replies to queries	Number of RIP responses

display rip database

Syntax

display rip *process-id* **database**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use the **display rip database** command to display the active routes in the RIP database, which are sent in normal RIP routing updates.

Examples

Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
   10.0.0.0/8, cost 6, ClassfulSumm
   10.0.0.0/8, cost 6, nexthop 192.168.0.37
   192.168.0.0/24, cost 0, ClassfulSumm
   192.168.0.0/24, cost 0, nexthop 192.168.0.73, Rip-interface
```

Table 1-2 display rip database command output description

Field	Description
X.X.X.X/X	Destination address and subnet mask
cost	Cost of the route
classful-summ	Indicates the route is a RIP summary route.
Nexthop	Address of the next hop
Rip-interface	Routes learnt from a RIP–enabled interface
imported	Routes redistributed from other routing protocols

display rip interface

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface.

Description

Use the **display rip interface** command to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

Examples

Display all the interface information of RIP process 1.

```
<Sysname> display rip 1 interface
Interface-name: Vlan-interface1
        Address/Mask:1.1.1.1/24        Version:RIPv1
        MetricIn:5     MetricIn route policy:123
        MetricOut:5    MetricOut route policy:234
        Split-horizon/Poison-reverse:on/off     Input/Output:on/on
        Default route:off
        Current packets number/Maximum packets number:234/2000
```

Table 1-3 display rip interface command output description

Field	Description
Interface-name	The name of an interface running RIP
Address/Mask	IP address and mask of the interface

Field	Description
Version	RIP version running on the interface
MetricIn	Additional routing metric added to the incoming routes
MetricIn route policy	Name of the routing policy used to add the additional routing metric for the incoming routes. If no routing policy is referenced, the field displays **Not designated**.
MetricOut	Additional routing metric added to the outgoing routes
MetricOut route policy	Name of the routing policy used to add the additional routing metric for the outgoing routes. If no routing policy is referenced, the field displays **Not designated**.
Split-horizon	Indicates whether split-horizon is enabled (ON: enabled, OFF: disabled)
Poison-reverse	Indicates whether poison-reverse is enabled (ON: enabled, OFF: disabled)
Input/Output	Indicates if the interface is allowed to receive (Input) or send (Output) RIP messages (on means it is allowed, off means it is not allowed)
Default route	Default route
Current packets number/Maximum packets number	Packets to be sent/Maximum packets that can be sent on the interface

display rip route

Syntax

display rip *process-id* **route** [**statistics** | *ip-address* { *mask* | *mask-length* } | **peer** *ip-address*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

statistics: Displays the route statistics, including total number of routes and number of routes of each neighbor.

ip-address { *mask* | *mask-length* }: Displays route information about a specified IP address.

peer *ip-address*: Displays all routing information learned from a specified neighbor.

Description

Use the **display rip route** command to display the routing information of a specified RIP process.

Examples

Display all routing information of RIP process 1.

```
<Sysname> display rip 1 route
```

```
 Route Flags: R-RIP, T-TRIP
              P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
------------------------------------------------------------------------------
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8          21.0.0.23      1        0       RA     102
34.0.0.0/8          21.0.0.23      1        0       RA      23
```

Display routing information for network 56.0.0.0/8 of RIP process 1.

```
<Sysname> display rip 1 route 56.0.0.0 8
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
------------------------------------------------------------------------------
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8          21.0.0.23      1        0       RA     102
```

Display RIP process1 routing information learned from the specified neighbor.

```
<Sysname> display rip 1 route peer 21.0.0.23
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
------------------------------------------------------------------------------
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8          21.0.0.23      1        0       RA        102
34.0.0.0/8          21.0.0.23      1        0       RA        23
```

Table 1-4 display rip route command output description

Field	Description
Route Flags	R — RIP route T — TRIP route P — The route never expires A — The route is aging S — The route is suppressed G — The route is in Garbage-collect state
Peer 21.0.0.23 on Vlan-interface1	Routing information learned on a RIP interface from the specified neighbor
Destination/Mask	Destination IP address and subnet mask
Nexthop	Next hop of the route
Cost	Cost of the route
Tag	Route tag
Flags	Indicates the route state
Sec	Remaining time of the timer corresponding to the route state

Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
```

```
Peer         Aging     Permanent    Garbage
21.0.0.23      2          0            3
21.0.0.12      2          0            4
Total          4          0            7
```

Table 1-5 display rip route statistics command output description

Field	Description
Peer	IP address of a neighbor
Aging	Total number of aging routes learned from the specified neighbor
Permanent	Total number of permanent routes learned from the specified neighbor
Garbage	Total number of routes in the garbage-collection state learned from the specified neighbor
Total	Total number of routes learned from all RIP neighbors

filter-policy export (RIP view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy export [*protocol* [*process-id*] | *interface-type interface-number*]

View

RIP view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter outbound routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: Name of an IP prefix list used to filter outbound routes, a string of 1 to 19 characters.

protocol: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

process-id: Process ID of the specified routing protocol, in the range of 1 to 65535. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

interface-type interface-number: Specifies an interface.

Description

Use the **filter-policy export** command to configure the filtering of RIP outgoing routes. Only routes not filtered out can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

By default, RIP does not filter outbound routes.

Note that:

- If *protocol* is specified, RIP filters only the outgoing routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.
- If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

Related commands: **acl**, **import-route**, and **ip ip-prefix**.

Examples

Reference ACL 2000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Reference IP prefix list **abc** to filter outbound routes on Vlan-interface 1.

```
[Sysname-rip-1] filter-policy ip-prefix abc export Vlan-interface 1
```

filter-policy import (RIP view)

Syntax

filter-policy { *acl-number* | **gateway** *ip-prefix-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

View

RIP view

Default Level

2: System level

Parameters

acl-number: Number of the ACL used for filtering incoming routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: References an IP prefix list to filter incoming routes. The *ip-prefix-name* is a string of 1 to 19 characters.

gateway *ip-prefix-name*: References an IP prefix list to filter routes from the gateway. *ip-prefix-name* is a string of 1 to 19 characters.

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

Description

Use the **filter-policy import** command to filter the incoming routes.

Use the **undo filter-policy import** command to restore the default.

By default, RIP does not filter incoming routes.

Related commands: **acl** and **ip ip-prefix**.

Examples

Reference ACL 2000 to filter incoming routes.

```
<Sysname> system-view
[Sysname] rip 1
```

```
[Sysname-rip-1] filter-policy 2000 import
```

Reference IP prefix list abc on Vlan-interface 1 to filter all received RIP routes.

```
[Sysname-rip-1] filter-policy ip-prefix abc import Vlan-interface 1
```

host-route

Syntax

host-route

undo host-route

View

RIP view

Default Level

2: System level

Parameters

None

Description

Use the **host-route** command to enable host route reception.

Use the **undo host-route** command to disable host route reception.

By default, receiving host routes is enabled.

In some cases, a router may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. You can use the **undo host-route** command to disable receiving of host routes.

 **Note**

RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

Examples

Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route (RIP view)

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route *protocol* [*process-id*]

View

RIP view

Default Level

2: System level

Parameters

protocol: Specifies a routing protocol from which to redistribute routes. At present, it can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **rip**, or **ospf**.

all-processes: Enables route redistribution from all the processes of a protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword. The **import-route bgp** command only redistributes eBGP routes, while the **import-route bgp allow-ibgp** command additionally redistributes iBGP routes, which may cause routing loops. Be cautious when using it.

cost: Cost for redistributed routes, in the range of 0 to 16. If *cost* is not specified, the default cost specified by the **default cost** command applies.

tag: Tag marking redistributed routes, in the range of 0 to 65,535. The default is 0.

route-policy *route-policy-name*: Specifies a routing policy with 1 to 19 characters.

Description

Use the **import-route** command to enable route redistribution from another routing protocol.

Use the **undo import-route** command to disable route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

Note that:

- Only active routes can be redistributed. You can use the display ip routing-table protocol command to display route state information.
- You can specify a routing policy using the keyword **route-policy** to redistribute only the specified routes.
- You can configure a cost for redistributed routes using the keyword **cost**.
- You can configure a tag value for redistributed routes using the keyword **tag**.

Related commands: **default cost**.

Examples

Redistribute static routes, and set the cost to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Set the default cost for redistributed routes to 3.

```
[Sysname-rip-1] default cost 3
```

Redistribute OSPF routes with the cost being the default cost.

```
[Sysname-rip-1] import-route ospf
```

maximum load-balancing (RIP view)

Syntax

maximum load-balancing *number*

undo maximum load-balancing

View

RIP view

Default Level

2: System level

Parameters

number: Maximum number of load balanced routes, in the range 1 to 4.

Description

Use the **maximum load-balancing** command to specify the maximum number of load balanced routes in load sharing mode.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of load balanced routes is 4.

Examples

Specify the maximum number of load balanced routes as 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

network

Syntax

network *network-address*

undo network *network-address*

View

RIP view

Default Level

2: System level

Parameters

network-address: IP address of a network segment, which can be the IP network address of any interface.

Description

Use the **network** command to enable RIP on the interface attached to the specified network.

Use the **undo network** command to disable RIP on the interface attached to the specified network.

Use the **network** 0.0.0.0 command to enable RIP on all interfaces.

RIP is disabled on an interface by default.

Note that:

- RIP runs only on the interfaces attached to the specified network. For an interface not on the specified network, RIP neither receives/sends routes on it nor forwards interface route through it. Therefore, you need to specify the network after enabling RIP to validate RIP on a specific interface.
- For a single process, you can use the network 0.0.0.0 command to enable RIP on all interfaces, while the command is not applicable in case of multi-process.
- If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

Enable RIP on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

output-delay

Syntax

output-delay *time* **count** *count*

undo output-delay

View

RIP view

Default Level

2: System level

Parameters

time: RIP packet sending interval, in milliseconds. It is in the range 10 to 100.

count: Maximum number of RIP packets sent at each interval. It is in the range 1 to 20.

Description

Use the **output-delay** command to configure the maximum RIP packets that can be sent at the specified interval for all interfaces under the RIP process.

Use the **undo output-delay** command to restore the default.

By default, an interface sends up to three RIP packets every 20 milliseconds.

Examples

Configure all the interfaces under RIP process 1 to send up to 10 RIP packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-1] output-delay 30 count 10
```

peer

Syntax

peer *ip-address*

undo peer *ip-address*

View

RIP view

Default Level

2: System level

Parameters

ip-address: IP address of a RIP neighbor, in dotted decimal format.

Description

Use the **peer** command to specify the IP address of a neighbor in the non-broadcast multi-access (NBMA) network, where routing updates destined for the peer are unicast, rather than multicast or broadcast.

Use the **undo peer** command to remove the IP address of a neighbor.

By default, no neighbor is specified.

Note that you need not use the **peer** *ip-address* command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.

Examples

Specify to send unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

preference

Syntax

preference [**route-policy** *route-policy-name*] *value*

undo preference [**route-policy**]

View

RIP view

Default Level

2: System level

Parameters

route-policy-name: Routing policy name with 1 to 19 characters.

value: Priority for RIP route, in the range of 1 to 255. The smaller the value, the higher the priority.

Description

Use the **preference** command to specify the RIP route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIP route is 100.

You can specify a routing policy using the keyword **route-policy** to set the specified priority to routes matching the routing policy.

- If a priority is set for matched routes in the routing policy, the priority applies to these routes. The priority of other routes is the one set by the **preference** command.
- If no priority is set for matched routes in the routing policy, the priority of all routes is the one set by the **preference** command.

Examples

Set the RIP route priority to 120.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip statistics

Syntax

reset rip *process-id* **statistics**

View

User view

Default Level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use the **reset rip statistics** command to clear the statistics of the specified RIP process.

Examples

Clear statistics in RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Syntax

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

View

System view

Default Level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 case-sensitive characters.

Description

Use the **rip** command to create a RIP process and enter RIP view.

Use the **undo rip** command to disable a RIP process.

By default, no RIP process runs.

Note that:

- If no VPN instance is specified, the RIP process will run under public network instance.
- You must create a VPN instance before you apply a RIP process to it. For related configuration, refer to the **ip vpn-instance** command.
- You must enable the RIP process before configuring the global parameters. This limitation is not for configuration of interface parameters.
- The configured interface parameters become invalid after you disable the RIP process.

Examples

Create a RIP process and enter RIP process view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Syntax

rip authentication-mode { **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } | **simple** *password* }

undo rip authentication-mode

View

Interface view

Default Level

2: System level

Parameters

md5: MD5 authentication mode.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

rfc2082: Uses the message format defined in RFC 2082.

key-id: MD5 key number, in the range of 1 to 255.

key-string: MD5 key string with 1 to 16 characters in plain text format, or 1 to 24 characters in cipher text format. When the **display current-configuration** command is used to display system information, a 24-character cipher string is displayed as the MD5 key string.

simple: Plain text authentication mode.

password: Plain text authentication string with 1 to 16 characters.

Description

Use the **rip authentication-mode** command to configure RIPv2 authentication mode and parameters.

Use the **undo rip authentication-mode** command to cancel authentication.

Note that the key string you configured can overwrite the old one if there is any.

Related commands: **rip version**.

Examples

Configure MD5 authentication on VLAN-interface 10 with the key string being **rose** in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 rose
```

rip default-route

Syntax

rip default-route { { **only** | **originate** } [**cost** *cost*] | **no-originate** }

undo rip default-route

View

Interface view

Default Level

2: System level

Parameters

only: Advertises only a default route.

originate: Advertises a default route and other routes.

no-originate: Advertises routes other than a default route.

cost: Cost of the default route, in the range 1 to 15.

Description

Use the **rip default-route** command to configure the RIP interface to advertise a default route with the specified metric.

Use the **undo rip default-route** command to disable the RIP interface from sending a default route.

By default, a RIP interface can advertise a default route if the RIP process is configured with default route advertisement.

Note

A RIP router configured to advertise a default route will not receive any default routes from RIP neighbors.

Related commands: **default-route**.

Examples

Configure VLAN-interface 10 to advertise only a default route with a metric of 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route only cost 2
```

rip input

Syntax

rip input

undo rip input

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip input** command to enable the interface to receive RIP messages.

Use the **undo rip input** command to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Related commands: **rip output**.

Examples

Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

rip metricin

Syntax

rip metricin [**route-policy** *route-policy-name*] *value*

undo rip metricin

View

Interface view

Default Level

2: System level

Parameters

route-policy *route-policy-name*: Specifies the name of a routing policy used to add an additional metric for the routes matching it. The name is a string of 1 to 19 characters

value: Additional metric added to received routes, in the range of 0 to 16.

Description

Use the **rip metricin** command to configure the interface to add a metric to the routes it receives.

Use the **undo rip metricin** command to restore the default.

By default, the additional metric of a received route is 0.

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. Therefore, the metric of the route received on the configured interface is increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy, while routes not matching it is added with the metric specified in the **rip metricout** command. Note that, the **rip metricout** command does not support the **+** or – keyword (used to add or reduce a metric) specified in the **apply cost** command. For details about the **apply cost** command, refer to *Routing Policy Commands* in the *IP Routing Volume*.
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Related commands: **rip metricout**.

Examples

Configure VLAN-interface 10 to add a metric of 6 for incoming route 1.0.0.0/8 and to add a metric of 2 for other incoming routes.

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
```

```
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin route-policy abc 2
```

rip metricout

Syntax

rip metricout [**route-policy** *route-policy-name*] *value*

undo rip metricout

View

Interface view

Parameters

value: Additional metric of sent routes, in the range of 1 to 16.

Description

Use the **rip metricout** command to add a metric to sent routes.

Use the **undo rip metricout** command to restore the default.

By default, the additional metric for sent routes is 1.

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy, while routes not matching it is added with the metric specified in the **rip metricout** command. Note that, the **rip metricout** command does not support the **+** or – keyword (used to add or reduce a metric) specified in the **apply cost** command. For details about the **apply cost** command, refer to *Routing Policy Commands* in the *IP Routing Volume*.
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Related commands: **rip metricin**.

Examples

Configure VLAN-interface 10 to add a metric of 6 for the outgoing route 1.0.0.0/8 and to add a metric of 2 for other outgoing routes.

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout route-policy abc 2
```

rip mib-binding

Syntax

rip mib-binding *process-id*

undo rip mib-binding

View

System view

Default Level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use the **rip mib-binding** command to bind MIB operations with a specified RIP process, so that the RIP process can receive SNMP requests.

Use the **undo rip mib-binding** command to restore the default.

By default, MIB operations are bound to RIP process 1, that is, RIP process 1 is enabled to receive SNMP requests.

Examples

Configure RIP 100 to accept SNMP requests.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

Restore the default.

```
[Sysname] undo rip mib-binding
```

rip output

Syntax

rip output

undo rip output

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip output** command to enable the interface to send RIP messages.

Use the **undo rip output** command to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Related commands: **rip input**.

Examples

Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip poison-reverse

Syntax

rip poison-reverse

undo rip poison-reverse

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples

Enable the poison reverse function for RIP routing updates on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip split-horizon

Syntax

rip split-horizon

undo rip split-horizon

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

The split horizon function is enabled by default.

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure it is necessary to disable the split horizon function.

 **Note**

Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

Examples

Enable the split horizon function on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Syntax

rip summary-address *ip-address* { *mask* | *mask-length* }

undo rip summary-address *ip-address* { *mask* | *mask-length* }

View

Interface view

Default Level

2: System level

Parameters

ip-address: Destination IP address of summary route.

mask: Subnet mask of summary route, in dotted decimal format.

mask-length: Subnet mask length of summary route, in the range 0 to 32.

Description

Use the **rip summary-address** command to configure RIPv2 to advertise a summary route through the interface.

Use the **undo rip summary-address** command to remove the configuration.

Note that the summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

Examples

Advertise a local summary address on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

rip version

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

View

Interface view

Default Level

2: System level

Parameters

1: RIP version 1.

2: RIP version 2.

broadcast: Sends RIPv2 messages in broadcast mode.

multicast: Sends RIPv2 messages in multicast mode.

Description

Use the **rip version** command to specify a RIP version for the interface.

Use the **undo rip version** command to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIPv1 broadcasts and can receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts and unicasts.

If RIPv2 is specified with no sending mode configured, RIPv2 messages will be sent in multicast mode.

When RIPv1 runs on an interface, the interface will:

- Send RIPv1 broadcast messages
- Receive RIPv1 broadcast messages
- Receive RIPv1 unicast messages

When RIPv2 runs on the interface in broadcast mode, the interface will:

- Send RIPv2 broadcast messages
- Receive RIPv1 broadcast messages
- Receive RIPv1 unicast messages
- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

When RIPv2 runs on the interface in multicast mode, the interface will:

- Send RIPv2 multicast messages
- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

Examples

Configure VLAN-interface 10 to broadcast RIPv2 messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

silent-interface (RIP view)

Syntax

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View

RIP view

Default Level

2: System level

Parameters

all: Silents all interfaces.

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

Description

Use the **silent-interface** command to disable an interface or all interfaces from sending routing updates. That is, the interface only receives but does not send RIP messages.

Use the **undo silent-interface** command to restore the default.

By default, all interfaces are allowed to send routing updates.

Examples

Configure all VLAN interfaces to work in the silent state, and activate VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
```

```
[Sysname-rip-100] network 131.108.0.0
```

summary

Syntax

summary

undo summary

View

RIP view

Default Level

2: System level

Parameters

None

Description

Use the **summary** command to enable automatic RIPv2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use the **undo summary** command to disable automatic RIPv2 summarization so that all subnet routes can be broadcast.

By default, automatic RIPv2 summarization is enabled.

Enabling automatic RIPv2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version**.

Examples

Enable RIPv2 automatic summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] summary
```

timers

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View

RIP view

Default Level

2: System level

Parameters

garbage-collect-value: Garbage-collect timer time in seconds, in the range of 1 to 3600.

suppress-value: Suppress timer time in seconds, in the range of 0 to 3600.

timeout-value: Timeout timer time in seconds, in the range of 1 to 3600.

update-value: Update timer time in seconds, in the range of 1 to 3600.

Description

Use the **timers** command to configure RIP timers. By adjusting RIP timers, you can improve network performance.

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

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIP is controlled by the above four timers.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Note that:

- Generally, you are not recommended to change the default values of these timers.
- The time lengths of these timers must be kept consistent on all routers and access servers in the network.

Examples

Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30 respectively.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

validate-source-address

Syntax

validate-source-address

undo validate-source-address

View

RIP view

Default Level

2: System level

Parameters

None

Description

Use the **validate-source-address** command to enable the source IP address validation on incoming RIP routing updates.

Use the **undo validate-source-address** command to disable the source IP address validation.

The source IP address validation is enabled by default.

Generally, disabling the validation is not recommended.

Examples

Enable the source IP address validation on incoming messages.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] validate-source-address
```

version

Syntax

version { **1** | **2** }

undo version

View

RIP view

Default Level

2: System level

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Description

Use the **version** command to specify a global RIP version.

Use the **undo version** command to remove the configured global RIP version.

By default, if an interface has a RIP version specified, the RIP version takes effect; if it has no RIP version specified, it can send RIPv1 broadcasts, and receive RIPv1 broadcasts, RIPv1 unicasts, RIPv2 broadcasts, RIPv2 multicasts, and RIPv2 unicasts.

Note that:

- If an interface has an RIP version specified, the RIP version takes precedence over the global RIP version.

- If no RIP version is specified for the interface and the global version is RIPv1, the interface inherits RIPv1, and it can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts.
- If no RIP version is specified for the interface and the global version is RIPv2, the interface operates in the RIPv2 muticast mode, and it can send RIPv2 multicasts, and receive RIPv2 broadcasts, multicasts and unicasts.

Examples

Specify RIPv2 as the global RIP version.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

Table of Contents

1 OSPF Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

OSPF Configuration Commands

abr-summary (OSPF area view)

Syntax

abr-summary *ip-address* { *mask* | *mask-length* } [**advertise** | **not-advertise**] [**cost** *cost*]

undo abr-summary *ip-address* { *mask* | *mask-length* }

View

OSPF area view

Default Level

2: System level

Parameters

ip-address: Destination IP address of the summary route, in dotted decimal format.

mask: Mask of the IP address in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

advertise | **not-advertise**: Advertises the summary route or not. By default, the summary route is advertised.

cost *cost*: Specifies the cost of the summary route, in the range 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Description

Use the **abr-summary** command to configure a summary route on the area border router.

Use the **undo abr-summary** command to remove a summary route.

By default, no route summarization is configured on an ABR.

You can enable advertising the summary route or not, and specify a route cost.

This command is usable only on an ABR. Multiple contiguous networks may be available in an area, where you can summarize them into one network on the ABR for advertisement. The ABR advertises only the summary route to other areas.

With the **undo abr-summary** command used, summarized routes will be advertised.

Examples

Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area (OSPF view)

Syntax

area *area-id*

undo area *area-id*

View

OSPF view

Default Level

2: System level

Parameters

area-id: ID of an area, a decimal integer in the range 0 to 4294967295 that is translated into the IP address format by the system, or an IP address.

Description

Use the **area** command to create an area and enter area view.

Use the **undo area** command to remove a specified area.

No OSPF area is created by default.

Examples

Create Area 0 and enter Area 0 view

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary

Syntax

asbr-summary *ip-address* { *mask* | *mask-length* } [**tag** *tag* | **not-advertise** | **cost** *cost*] *

undo asbr-summary *ip-address* { *mask* | *mask-length* }

View

OSPF view

Default Level

2: System level

Parameters

ip-address: IP address of the summary route in dotted decimal notation.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range 0 to 32 bits.

not-advertise: Disables advertising the summary route. If the keyword is not specified, the route is advertised.

tag *tag*: Specifies a tag value for the summary route, used by a route policy to control summary route advertisement, in the range 0 to 4294967295. The default is 1.

cost *cost*: Specifies the cost of the summary route, in the range 1 to 16777214. For Type-1 external routes, the cost defaults to the largest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the largest cost among routes that are summarized plus 1.

Description

Use the **asbr-summary** command to configure a summary route.

Use the **undo asbr-summary** command to remove a summary route.

No ASBR route summarization is configured by default.

With the **asbr-summary** command configured on an ASBR, it summarizes redistributed routes that fall into the specified address range into a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured on an NSSA ABR, it summarizes routes described by Type-5 LSAs translated from Type-7 LSAs into a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

With the **undo asbr-summary** command used, summarized routes will be advertised.

Related command: **display ospf asbr-summary**.

Examples

Summarize redistributed routes into a single route, specifying a tag value of 2 and a cost of 100 for the summary route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Syntax

authentication-mode { **simple** | **md5** }

undo authentication-mode

View

OSPF area view

Default Level

2: System level

Parameters

simple: Specifies the simple authentication mode.

md5: Specifies the MD5 ciphertext authentication mode.

Description

Use the **authentication-mode** command to specify an authentication mode for the OSPF area.

Use the **undo authentication-mode** command to remove the authentication mode.

By default, no authentication mode is configured for an OSPF area.

Routers that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode**.

Examples

Configure OSPF area 0 to use the MD5 ciphertext authentication mode.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

bandwidth-reference (OSPF view)

Syntax

bandwidth-reference *value*

undo bandwidth-reference

View

OSPF view

Default Level

2: System level

Parameters

value: Bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

Description

Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values: Cost=Reference bandwidth value / Link bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

Examples

Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

default

Syntax

default { **cost** *cost* | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

View

OSPF view

Default Level

2: System level

Parameters

cost: Specifies the default cost for redistributed routes, in the range 0 to 16777214.

limit: Specifies the default upper limit of routes redistributed per time, in the range 1 to 2147483647.

tag: Specifies the default tag for redistributed routes, in the range 0 to 4294967295.

type: Specifies the default type for redistributed routes: 1 or 2.

Description

Use the **default** command to configure default parameters for redistributed routes.

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

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route**.

Examples

Configure the default cost, upper limit, tag and type as 10, 20000, 100 and 2 respectively for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

default-cost (OSPF area view)

Syntax

default-cost *cost*

undo default-cost

View

OSPF area view

Default Level

2: System level

Parameters

cost: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range 0 to 16777214.

Description

Use the **default-cost** command to configure a cost for the default route advertised to the stub or NSSA area.

Use the **undo default-cost** command to restore the default value.

The cost defaults to 1.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub**, **nssa**.

Examples

Configure Area 1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

default-route-advertise (OSPF view)

Syntax

default-route-advertise [[**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] * | **summary cost** *cost*]

undo default-route-advertise

View

OSPF view

Default Level

2: System level

Parameters

always: Generates a default route in an ASE LSA into the OSPF routing domain regardless of whether a default route exists in the routing table. Without this keyword used, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain only when a default route exists in the routing table.

cost *cost*: Specifies a cost for the default route, in the range 0 to 16777214. If no *cost* is specified, the default cost specified by the **default cost** command applies..

type *type*: Specifies a type for the ASE LSA: 1 or 2. If *type* is not specified, the default type for the ASE LSA specified by the **default type** command applies..

route-policy *route-policy-name*: Specifies a route policy name, a string of 1 to 19 characters. If the default route matches the specified route policy, the route policy modifies some values in the ASE LSA.

summary: Advertises the Type-3 summary LSA of the specified default route.

Description

Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from distributing a default external route.

By default, no default route is distributed.

Using the **import-route** command cannot redistribute a default route. To do so, use the **default-route-advertise** command. If no default route exists in the router's routing table, use the **default-route-advertise always** command to generate a default route in a Type-5 LSA.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE router advertises the redistributed default route to the CE router.

Related commands: **import-route**, **default**.

Examples

Generate a default route in an ASE LSA into the OSPF routing domain (no default route configured on the router), regardless of whether the default route is available in the routing table.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

description (OSPF/OSPF area view)

Syntax

description *description*

undo description

View

OSPF view/OSPF area view

Default Level

2: System level

Parameters

description: Configures a description for the OSPF process in OSPF view, or for the OSPF area in OSPF area view. *description* is a string of up to 80 characters.

Description

Use the **description** command to configure a description for an OSPF process or area.

Use the **undo description** command to remove the description.

No description is configured by default.

Use of this command is only for the identification of an OSPF process or area. The description has no special meaning.

Examples

Describe the OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Describe the OSPF area0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

display ospf abr-asbr

Syntax

display ospf [*process-id*] **abr-asbr**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535. Use this argument to display information about the routes to the ABR/ASBR under the specified OSPF process.

Description

Use the **display ospf abr-asbr** command to display information about the routes to OSPF ABR/ASBR.

If you use this command on routers in a stub area, no ASBR information is displayed.

Examples

Display information about the routes to the OSPF ABR and ASBR.

```
<Sysname> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                 Routing Table to ABR and ASBR

Type        Destination       Area       Cost  Nexthop         RtType
Inter       3.3.3.3           0.0.0.0    3124  10.1.1.2        ASBR
Intra       2.2.2.2           0.0.0.0    1562  10.1.1.2        ABR
```

Table 1-1 display ospf abr-asbr command output description

Field	Description
Type	Type of the route to the ABR or ASBR: • Intra: intra-area route • Inter: Inter-area route
Destination	Router ID of an ABR/ASBR
Area	ID of the area of the next hop
Cost	Cost from the router to the ABR/ASBR
Nexthop	Next hop address
RtType	Router type: ABR, ASBR

display ospf asbr-summary

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask* | *mask-length* }]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

ip-address: IP address, in dotted decimal format.

mask: IP address mask, in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

Description

Use the **display ospf asbr-summary** command to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

Examples

Display information about all summarized redistributed routes.

```
<Sysname> display ospf asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  Summary Addresses

 Total Summary Address Count: 1

                  Summary Address

 Net         : 30.1.0.0
 Mask        : 255.255.0.0
 Tag         : 20
 Status      : Advertise
 Cost        : 10 (Configured)
 The Count of Route is : 2

 Destination     Net Mask        Proto      Process   Type     Metric

 30.1.2.0        255.255.255.0   OSPF       1         2        1
 30.1.1.0        255.255.255.0   OSPF       1         2        1
```

Table 1-2 display ospf asbr-summary command output description

Field	Description
Total Summary Address Count	Total summary route number
Net	The address of the summary route
Mask	The mask of the summary route address
Tag	The tag of the summary route
Status	The advertisement status of the summary route
Cost	The cost to the summary net
The Count of Route	The count of routes that are summarized
Destination	Destination address of a summarized route
Net Mask	Network mask of a summarized route
Proto	Routing protocol
Process	Process ID of routing protocol
Type	Type of a summarized route
Metric	Metric of a summarized route

display ospf brief

Syntax

display ospf [*process-id*] **brief**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf brief** command to display OSPF brief information. If no OSPF process is specified, brief information about all OSPF processes is displayed.

Examples

Display OSPF brief information.

```
<Sysname> display ospf brief

          OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

 RouterID: 192.168.1.2      Border Router:  NSSA
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 Applications Supported: MPLS Traffic-Engineering
 SPF-schedule-interval: 5 0 5000
 LSA generation interval: 5 0 5000
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route Preference: 10
 ASE Route Preference: 150
 SPF Computation Count: 22
 RFC 1583 Compatible
 Area Count: 1   Nssa Area Count: 1
 ExChange/Loading Neighbors: 0


 Area: 0.0.0.1          (MPLS TE  not enabled)
 Authtype: None Area flag: NSSA
 SPF Scheduled Count: 5
 ExChange/Loading Neighbors: 0
```

```
Interface: 192.168.1.2 (Vlan-interface1)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated Router: 192.168.1.2
Backup Designated Router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Delay 1
```

Table 1-3 display ospf brief command output description

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID
RouterID	Router ID
Border Router	Whether the router is a boarder router: • ABR • ASBR • NSSA ABR
Route Tag	The tag of redistributed routes
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
Applications Supported	Applications supported. MPLS Traffic-Engineering means MPLS TE is supported.
SPF-schedule-interval	Interval for SPF calculations
LSA generation interval	LSA generation interval
LSA arrival interval	Minimum LSA repeat arrival interval
Transmit pacing	LSU packet transmit rate of the interface: • **Interval** indicates the LSU transmit interval of the interface. • **Count** indicates the maximum number of LSU packets sent during each interval.
Default ASE Parameter	Default ASE Parameters: metric, tag, route type.
Route Preference	Internal route priority
ASE Route Preference	External route priority
SPF Computation count	SPF computation count of the OSPF process
RFC1583 Compatible	Compatible with routing rules defined in RFC1583
Area Count	Area number of the current process
Nssa Area Count	NSSA area number of the current process
ExChange/Loading Neighbors	Neighbors in ExChange/Loading state
Area	Area ID in the IP address format
Authtype	Authentication type of the area: • None: Non-authentication • Simple: simple authentication • MD5: MD5 authentication
Area flag	The type of the area
SPF scheduled Count	SPF calculation count in the OSPF area

Field	Description
Interface	Interface in the area
Cost	Interface cost
State	Interface state
Type	Interface network type
MTU	Interface MTU
Priority	Router priority
Designated Router	The Designated Router
Backup Designated Router	The Backup Designated Router
Timers	Intervals of timers: hello, dead, poll, retransmit, and transmit delay

display ospf cumulative

Syntax

display ospf [*process-id*] **cumulative**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf cumulative** command to display OSPF statistics.

Use of this command is helpful for troubleshooting.

Examples

Display OSPF statistics.

```
<Sysname> display ospf cumulative
          OSPF Process 1 with Router ID 2.2.2.2
                  Cumulations

  IO Statistics
              Type        Input     Output
             Hello           61        122
   DB Description            2          3
   Link-State Req            1          1
Link-State Update            3          3
   Link-State Ack            3          2
```

```
LSAs originated by this router
Router: 4
Network: 0
Sum-Net: 0
Sum-Asbr: 0
External: 0
NSSA: 0
Opq-Link: 0
Opq-Area: 0
Opq-As: 0

LSAs Originated: 4  LSAs Received: 7

Routing Table:
  Intra Area: 2  Inter Area: 3  ASE/NSSA: 0
```

Table 1-4 display ospf cumulative command output description

Field	Description
IO statistics	Statistics about input/output packets and LSAs
Type	OSPF packet type
Input	Packets received
Output	Packets sent
Hello	Hell packet
DB Description	Database Description packet
Link-State Req	Link-State Request packet
Link-State Update	Link-State Update packet
Link-State Ack	Link-State Acknowledge packet
LSAs originated by this router	LSAs originated by this router
Router	Number of Type-1 LSAs originated
Network	Number of Type-2 LSAs originated
Sum-Net	Number of Type-3 LSAs originated
Sum-Asbr	Number of Type-4 LSAs originated
External	Number of Type-5 LSAs originated
NSSA	Number of Type-7 LSAs originated
Opq-Link	Number of Type-9 LSAs originated
Opq-Area	Number of Type-10 LSAs originated
Opq-As	Number of Type-11 LSAs originated
LSA originated	Number of LSAs originated
LSA Received	Number of LSAs received
Routing Table	Routing table information

Field	Description
Intra Area	Intra-area route number
Inter Area	Inter-area route number
ASE	ASE route number

display ospf error

Syntax

display ospf [*process-id*] **error**

View

Anyview

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf error** command to display OSPF error information.

If no process is specified, the OSPF error information of all OSPF processes is displayed.

Examples

Display OSPF error information.

```
<Sysname> display ospf error

          OSPF Process 1 with Router ID 192.168.80.100
                 OSPF Packet Error Statistics

0    : OSPF Router ID confusion     0    : OSPF bad packet
0    : OSPF bad version             0    : OSPF bad checksum
0    : OSPF bad area ID             0    : OSPF drop on unnumber interface
0    : OSPF bad virtual link        0    : OSPF bad authentication type
0    : OSPF bad authentication key  0    : OSPF packet too small
0    : OSPF Neighbor state low      0    : OSPF transmit error
0    : OSPF interface down          0    : OSPF unknown neighbor
0    : HELLO: Netmask mismatch      0    : HELLO: Hello timer mismatch
0    : HELLO: Dead timer mismatch   0    : HELLO: Extern option mismatch
0    : HELLO: NBMA neighbor unknown 0    : DD: MTU option mismatch
0    : DD: Unknown LSA type         0    : DD: Extern option mismatch
0    : LS ACK: Bad ack              0    : LS ACK: Unknown LSA type
0    : LS REQ: Empty request        0    : LS REQ: Bad request
0    : LS UPD: LSA checksum bad     0    : LS UPD: Received less recent LSA
0    : LS UPD: Unknown LSA type
```

Table 1-5 display ospf error command output description

Field	Description
OSPF Router ID confusion	Packets with duplicate route ID
OSPF bad packet	Packets illegal
OSPF bad version	Packets with wrong version
OSPF bad checksum	Packets with wrong checksum
OSPF bad area ID	Packets with invalid area ID
OSPF drop on unnumber interface	Packets dropped on the unnumbered interface
OSPF bad virtual link	Packets on wrong virtual links
OSPF bad authentication type	Packets with invalid authentication type
OSPF bad authentication key	Packets with invalid authentication key
OSPF packet too small	Packets too small in length
OSPF Neighbor state low	Packets received in low neighbor state
OSPF transmit error	Packets with error when being transmitted
OSPF interface down	Shutdown times of the interface
OSPF unknown neighbor	Packets received from unknown neighbors
HELLO: Netmask mismatch	Hello packets with mismatched mask
HELLO: Hello timer mismatch	Hello packets with mismatched hello timer
HELLO: Dead timer mismatch	Hello packets with mismatched dead timer
HELLO: Extern option mismatch	Hello packets with mismatched option field
HELLO: NBMA neighbor unknown	Hello packets received from unknown NBMA neighbors
DD: MTU option mismatch	DD packets with mismatched MTU
DD: Unknown LSA type	DD packets with unknown LSA type
DD: Extern option mismatch	DD packets with mismatched option field
LS ACK: Bad ack	Bad LSAck packets for LSU packets
LS ACK: Unknown LSA type	LSAck packets with unknown LSA type
LS REQ: Empty request	LSR packets with no request information
LS REQ: Bad request	Bad LSR packets
LS UPD: LSA checksum bad	LSU packets with wrong LSA checksum
LS UPD: Received less recent LSA	LSU packets without latest LSA
LS UPD: Unknown LSA type	LSU packets with unknown LSA type

display ospf interface

Syntax

display ospf [*process-id*] **interface** [**all** | *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

all: Display the OSPF information of all interfaces.

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

Description

Use the **display ospf interface** command to display OSPF interface information.

If no OSPF process is specified, the OSPF interface information of all OSPF processes is displayed.

Examples

Display OSPF interface information.

```
<Sysname> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     PTP          P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type         State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast    DR       1     1     172.16.0.1      0.0.0.0
```

Table 1-6 display ospf interface command output description

Field	Description
Area	Area ID of the interface
IP address	Interface IP address (regardless of whether TE is enabled or not)
Type	Interface network type: PTP, PTMP, Broadcast, or NBMA

Field	Description
State	Interface state defined by interface state machine: • DOWN: In this state, no protocol traffic will be sent or received on the interface. • Waiting: Means the interface starts sending and receiving Hello packets and the router is trying to determine the identity of the (Backup) designated router for the network. • p-2-p: Means the interface will send Hello packets at the interval of HelloInterval, and try to establish an adjacency with the neighbor. • DR: Means the router itself is the designated router on the attached network. • BDR: Means the router itself is the backup designated router on the attached network. • DROther: Means the interface is on a network on which another router has been selected as the designated router.
Cost	Interface cost
Pri	Router priority
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment

display ospf lsdb

Syntax

display ospf [*process-id*] **lsdb** [**brief** | [{ **ase** | **router** | **network** | **summary** | **asbr** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** *advertising-router-id* | **self-originate**]]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

brief: Displays brief LSDB information.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

opaque-area: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

link-state-id: Link state ID, in the IP address format.

originate-router *advertising-router-id*: Displays information about LSAs originated by the specified router.

self-originate: Displays information about self-originated LSAs.

Description

Use the **display ospf lsdb** command to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

Examples

Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter         Age  Len   Sequence   Metric
 Router    192.168.0.2     192.168.0.2       474  36    80000004       0
 Router    192.168.0.1     192.168.0.1        21  36    80000009       0
 Network   192.168.0.1     192.168.0.1       321  32    80000003       0
 Sum-Net   192.168.1.0     192.168.0.1       321  28    80000002       1
 Sum-Net   192.168.2.0     192.168.0.2       474  28    80000002       1
                         Area: 0.0.0.1
 Type      LinkState ID    AdvRouter         Age  Len   Sequence   Metric
 Router    192.168.0.1     192.168.0.1        21  36    80000005       0
 Sum-Net   192.168.2.0     192.168.0.1       321  28    80000002       2
 Sum-Net   192.168.0.0     192.168.0.1       321  28    80000002       1
```

Table 1-7 display ospf lsdb command output description

Field	Description
Area	LSDB information of the area
Type	LSA type
LinkState ID	Linkstate ID
AdvRouter	The router that advertised the LSA
Age	Age of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost of the LSA

Display Type2 LSA (Network LSA) information in the LSDB.

```
<Sysname> display ospf 1 lsdb network

          OSPF Process 1 with Router ID 192.168.1.1
                      Area: 0.0.0.0
```

```
              Link State Database

Type      : Network
LS ID     : 192.168.0.2
Adv Rtr   : 192.168.2.1
LS Age    : 922
Len       : 32
Options   :  E
Seq#      : 80000003
Chksum    : 0x8d1b
Net Mask  : 255.255.255.0
   Attached Router    192.168.1.1
   Attached Router    192.168.2.1
                      Area: 0.0.0.1
              Link State Database
Type      : Network
LS ID     : 192.168.1.2
Adv Rtr   : 192.168.1.2
LS Age    : 782
Len       : 32
Options   :  NP
Seq#      : 80000003
Chksum    : 0x2a77
Net Mask  : 255.255.255.0
   Attached Router    192.168.1.1
   Attached Router    192.168.1.2
```

Table 1-8 display ospf 1 lsdb network command output description

Field	Description
Type	LSA type
LS ID	DR IP address
Adv Rtr	Router that advertised the LSA
LS Age	LSA age time
Len	LSA length
Options	LSA options: O: Opaque LSA advertisement capability E: AS External LSA reception capability EA: External extended LSA reception capability DC: On-demand link support N: NSSA external LSA support P: Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Seq#	LSA sequence number
Chksum	LSA checksum
Net Mask	Network mask
Attached Router	ID of the router that established adjacency with the DR, and ID of the DR itself

display ospf nexthop

Syntax

display ospf [*process-id*] **nexthop**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf nexthop** command to display OSPF next hop information.

If no OSPF process is specified, the next hop information of all OSPF processes is displayed.

Examples

Display OSPF next hop information.

```
<Sysname> display ospf nexthop
         OSPF Process 1 with Router ID 192.168.0.1
                 Routing Nexthop Information
```

```
 Next Hops:
 Address         Refcount  IntfAddr        Intf Name
-----------------------------------------------------------------
 192.168.0.1     1         192.168.0.1     Vlan-interface1
 192.168.0.2     1         192.168.0.1     Vlan-interface1
 192.168.1.1     1         192.168.1.1     Vlan-interface10
```

Table 1-9 display ospf nexthop command output description

Field	Description
Next hops	Information about Next hops
Address	Next hop address
Refcount	Reference count, namely, routes that reference the next hop
IntfAddr	Outbound interface address
Intf Name	Outbound interface name

display ospf peer

Syntax

display ospf [*process-id*] **peer** [**verbose |** [*interface-type interface-number*] [*neighbor-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

verbose: Displays detailed neighbor information.

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

neighbor-id: Neighbor router ID.

Description

Use the **display ospf peer** command to display information about OSPF neighbors.

Note that:

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF processes is displayed.

Examples

Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2          GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
   Dead timer due in 33  sec
   Neighbor is up for 02:03:35
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
```

Table 1-10 display ospf peer verbose command output description

Field	Description
Area *areaID* interface *IPAddress*(*InterfaceName*)'s neighbors	Neibghor information of the interface in the specified area: • *areaID*: Area to which the neighbor belongs. • *IPAddress*: Initerface IP address • *InterfaceName*: Interface name
interface	Interface attached with the neighbor
Router ID	Neighbor router ID
Address	Neighbor router address
GR State	GR state
State	Neighbor state: • Down: This is the initial state of a neighbor conversation. • Init: In this state, the router has seen a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor (the router itself did not appear in the neighbor's hello packet). • Attempt: Available only in an NBMA network, Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets with a longer interval to keep neighbor relationship. • 2-Way: In this state, communication between the two routers is bidirectional. The router itself appears in the neighbor's Hello packet. • Exstart: The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. • Exchange: In this state, the router is sending DD packets to the neighbor, describing its entire link-state database. • Loading: In this state, the router sends Link State Request packets to the neighbor, requesting more recent LSAs. • Full: In this state, the neighboring routers are fully adjacent.
Mode	Neighbor mode for LSDB synchronization: • Nbr is Master: Means the neighboring router is the master. • Nbr is Slave: Means the neighboring router is the slave.
Priority	Neighboring router priority
DR	The DR on the interface’s network segment

Field	Description
BDR	The BDR on the interface's network segment
MTU	Interface MTU
Dead timer due in 33 sec	Dead timer times out in 33 seconds
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication Sequence	Authentication sequence number
Neighbor state change count	Count of neighbor state changes

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer

                  OSPF Process 1 with Router ID 1.1.1.1
                       Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time Interface       State
 1.1.1.2         1.1.1.2         1   40         Vlan1        Full/DR
```

Table 1-11 display ospf peer command output description

Field	Description
Area	Neighbor area
Router ID	Neighbor router ID
Address	Neighbor interface address
Pri	Neighboring router priority
Dead time(s)	Dead interval remained
Interface	Interface connected to the neighbor
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full

display ospf peer statistics

Syntax

display ospf [*process-id*] **peer statistics**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf peer statistics** command to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

Examples

Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
          OSPF Process 1 with Router ID 10.3.1.1
                    Neighbor Statistics
  Area ID         Down Attempt Init 2-Way ExStart Exchange Loading Full Total
  0.0.0.0         0    0       0    0     0       0        0       1    1
  0.0.0.2         0    0       0    0     0       0        0       1    1
  Total           0    0       0    0     0       0        0       2    2
```

Table 1-12 d**isplay ospf peer statistics** command output description

Field	Description
Area ID	Area ID. The state statistics information of all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in the Down state in the same area
Attempt	Number of neighboring routers in the Attempt state in the same area
Init	Number of neighboring routers in the Init state in the same area
2-Way	Number of neighboring routers in the 2-Way state in the same area
ExStart	Number of neighboring routers in the ExStart state in the same area
Exchange	Number of neighboring routers in the Exchange state in the same area
Loading	Number of neighboring routers in the Loading state in the same area
Full	Number of neighboring routers in the Full state in the same area
Total	Total number of neighbors under the same state, namely, Down, Attempt, Init, 2-Way, ExStart, Loading, or Full.

display ospf request-queue

Syntax

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

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

neighbor-id: Neighbor's router ID.

Description

Use the **display ospf request-queue** command to display OSPF request queue information.

If no OSPF process is specified, the OSPF request queue information of all OSPF processes is displayed.

Examples

Display OSPF request queue information.

```
<Sysname> display ospf request-queue

          OSPF Process 1 with Router ID 1.1.1.1
                  OSPF Request List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Request list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           1.1.1.1           80000004   1
       Network    192.168.0.1       1.1.1.1         80000003   1
       Sum-Net    192.168.1.0       1.1.1.1             80000002   2
```

Table 1-13 display ospf request queue command output description

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Local interface IP address
Area	Area ID
Request list	Request list information
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

display ospf retrans-queue

Syntax

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

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

neighbor-id: Neighbor's router ID.

Description

Use the **display ospf retrans-queue** command to display retransmission queue information.

If no OSPF process is specified, the retransmission queue information of all OSPF processes is displayed.

Examples

Display OSPF retransmission queue information.

```
<Sysname> display ospf retrans-queue

         OSPF Process 1 with Router ID 1.1.1.1
                 OSPF Retransmit List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           2.2.2.2           80000004   1
       Network    12.18.0.1         2.2.2.2         80000003   1
       Sum-Net    12.18.1.0         2.2.2.2             80000002   2
```

Table 1-14 display ospf retrans-queue command output description

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Interface address of the router
Area	Area ID
Retrans List	Retransmission list
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

display ospf routing

Syntax

display ospf [*process-id*] **routing** [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

interface *interface-type interface-number*: Displays OSPF routing information advertised via the interface.

nexthop *nexthop-address*: Displays OSPF routing information with the specified next hop.

Description

Use the **display ospf routing** command to display OSPF routing information.

If no OSPF process is specified, the routing information of all OSPF processes is displayed.

Examples

Display OSPF routing information.

```
<Sysname> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter     Area
 192.168.1.0/24     1562  Stub       192.168.1.2     192.168.1.2   0.0.0.0
 172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1   0.0.0.0

 Total Nets: 2
 Intra Area: 1  Inter Area: 1  ASE: 0  NSSA: 0
```

Table 1-15 display ospf routing command output description

Field	Description
Destination	Destination network
Cost	Cost to destination
Type	Route type: intra-area, transit, stub, inter-area, type1 external, type2 external.
NextHop	Next hop address
AdvRouter	Advertising router
Area	Area ID

Field	Description
Total Nets	Total networks
Intra Area	Total intra-area routes
Inter Area	Total inter-area routes
ASE	Total ASE routes
NSSA	Total NSSA routes

display ospf vlink

Syntax

display ospf [*process-id*] **vlink**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **display ospf vlink** command to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

Examples

Display OSPF virtual link information.

```
<Sysname> display ospf vlink
          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (Vlan-interface1)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 1-16 display ospf vlink command output description

Field	Description
Virtual-link Neighbor-id	ID of the neighbor connected to the router via the virtual link
Neighbor-State	Neighbor State: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	Local interface’s IP address and name of the virtual link
Cost	Interface route cost

Field	Description
State	Interface state
Type	Type: virtual link
Transit Area	Transit area ID
Timers	Values of timers: hello, dead, poll (NBMA), retransmit, and interface transmission delay

enable link-local-signaling

Syntax

enable link-local-signaling

undo enable link-local-signaling

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **enable link-local-signaling** command to enable the OSPF link-local signaling (LLC) capability.

Use the **undo enable link-local-signaling** command to disable the OSPF link-local signaling capability.

By default, this capability is disabled.

Examples

Enable link-local signaling for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable log

Syntax

enable log [**config** | **error** | **state**]

undo enable log [**config** | **error** | **state**]

View

OSPF view

Default Level

2: System level

Parameters

config: Enables configuration logging.

error: Enables error logging.

state: Enables state logging.

Description

Use the **enable** command to enable specified OSPF logging.

Use the **undo enable** command to disable specified OSPF logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

Examples

Enable OSPF logging.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

enable out-of-band-resynchronization

Syntax

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **enable out-of-band-resynchronization** command to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use the **undo enable out-of-band-resynchronization** command to disable the OSPF out-of-band resynchronization capability.

By default, the capability is disabled.

Examples

Enable the out-of-band resynchronization capability for OSPF process 1.

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

```
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

filter

Syntax

filter { *acl-number* | **ip-prefix** *ip-prefix-name* } { **import** | **export** }

undo filter { **import** | **export** }

View

OSPF area view

Default Level

2: System level

Parameters

acl-number: ACL number, in the range 2000 to 3999.

ip-prefix-name: IP prefix list name, a string of up to 19 characters. For details about IP prefix lists, see *Route Policy Configuration* in the *IP Routing Volume*.

import: Filters Type-3 LSAs advertised into the area.

export: Filters Type-3 LSAs advertised to other areas.

Description

Use the **filter** command to configure incoming/outgoing Type-3 LSAs filtering on an ABR.

Use the **undo filter** command to disable Type-3 LSA filtering.

By default, Type-3 LSAs filtering is disabled.

Note

This command is only available on an ABR.

Examples

Apply IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs, and apply ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPF view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View

OSPF view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter redistributed routes, in the range 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter redistributed routes, a string of up to 19 characters.

protocol: Specifies a protocol from which to filter redistributed routes. The protocol can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

process-id: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

Description

Use the **filter-policy export** command to configure the filtering of redistributed routes.

Use the **undo filter-policy export** command to disable the filtering.

By default, the filtering of redistributed routes is not configured.

You can use this command to filter redistributed routes as needed.

Related commands: **import-route**.

Examples

Filter redistributed routes using ACL2000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

filter-policy import (OSPF view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

undo filter-policy import

View

OSPF view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter incoming routes, in the range 2000 to 3999.

ip-prefix-name: Name of an IP address prefix list used to filter incoming routes based on destination IP address, a string of up to 19 characters. For details about IP prefix lists, refer to *Route Policy Configuration* in the *IP Routing Volume*.

gateway *ip-prefix-name*: Name of an IP address prefix list used to filter routes based on the next hop of the routing information, a string of up to 19 characters.

Description

Use the **filter-policy import** command to configure the filtering of routes calculated from received LSAs.

Use the **undo filter-policy import** command to disable the filtering.

By default, the filtering is not configured.

Examples

Filter incoming routes using ACL2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

graceful-restart (OSPF view)

Syntax

graceful-restart [**nonstandard** | **ietf**]

undo graceful-restart

View

OSPF view

Default Level

2: System level

Parameters

nonstandard: Enables the non-IETF GR capability.

ietf: Enables the IETF GR capability.

Description

Use the **graceful-restart** command to enable OSPF Graceful Restart capability.

Use the **undo graceful-restart** command to disable OSPF Graceful Restart capability.

By default, OSPF Graceful Restart capability is disabled.

Note the following:

- Enable Opaque LSA advertisement and reception with the **opaque-capability enable** command before enabling the IETF GR capability for OSPF.
- Before enabling non-IETF GR capability for OSPF, enable OSPF LLS (link local signaling) with the **enable link-local-signaling** command and OOB (out of band resynchronization) with the **enable out-of-band-resynchronization** command.
- If the keywords **nonstandard** and **ietf** are not specified when OSPF GR is enabled, **nonstandard** is the default.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**, **opaque-capability enable**.

Examples

Enable IETF Graceful Restart for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf
```

Enable non-IETF Graceful Restart for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

graceful-restart help

Syntax

graceful-restart help { *acl-number* | **prefix** *prefix-list* }

undo graceful-restart help

View

OSPF view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range 2000 to 3999.

prefix-list: Name of the specified IP prefix list, a string of 1 to 19 characters.

Description

Use the **graceful-restart help** command to configure for which OSPF neighbors the current router can serve as a GR Helper. (The neighbors are specified by the ACL or the IP prefix list.)

Use the **undo graceful-restart help** command to restore the default.

By default, the router can serve as a GR Helper for any OSPF neighbor.

Examples

Enable IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF neighbors defined in the ACL 2001.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart help 2001
```

Enable non IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF neighbors defined in the ACL 2001.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart help 2001
```

graceful-restart interval (OSPF view)

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

View

OSPF view

Default Level

2: System level

Parameters

interval-value: Specifies the Graceful Restart interval, in the range 40 to 1,800 seconds.

Description

Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 120 seconds.

Note that the Graceful Restart interval of OSPF cannot be less than the maximum value of dead intervals on all OSPF interfaces; otherwise, the Graceful Restart of OSPF may fail.

Related commands: **ospf timer dead**.

Examples

Configure the Graceful Restart interval for OSPF process 1 as 100 seconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

host-advertise

Syntax

host-advertise *ip-address cost*

undo host-advertise *ip-address*

View

OSPF area view

Default Level

2: System level

Parameters

ip-address: IP address of a host

cost: Cost of the route, in the range 1 to 65535.

Description

Use the **host-advertise** command to advertise a host route.

Use the **undo host-advertise** command to remove a host route.

No host route is advertised by default.

Examples

Advertise route 1.1.1.1 with a cost of 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]host-advertise 1.1.1.1 100
```

import-route (OSPF view)

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id* | **all-processes**]

View

OSPF view

Default Level

2: System level

Parameters

protocol: Redistributes routes from the specified protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the *protocol* is **rip**, **ospf**, or **isis**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows IBGP routes redistribution. It is optional only when the *protocol* is **bgp**.

cost *cost*: Specifies a route cost, in the range 0 to 16777214. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

tag *tag* : Specifies a tag for external LSAs. The default is 1.

route-policy *route-policy-name*: Specifies a route policy to redistribute qualified routes only. A Route policy name is a string of up to 19 characters.

Description

Use the **import-route** command to redistribute routes from another protocol.

Use the **undo import-route** command to disable route redistribution from a protocol.

Route redistribution from another protocol is not configured by default.

OSPF prioritize routes as follows:

- Intra-area route
- Inter-area route
- Type1 External route
- Type2 External route

An intra-area route is a route in an OSPF area. An inter-area route is between any two OSPF areas. Both of them are internal routes.

An external route is a route to a destination outside the OSPF AS.

A Type-1 external route is an IGP route, such as RIP or STATIC, which has high reliability and whose cost is comparable with the cost of OSPF internal routes. Therefore, the cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the corresponding ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route is an EGP route, which has low credibility, so OSPF considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

Related commands: **default-route-advertise.**

Note

- The **import-route** command cannot redistribute default routes.
- Use the **import-route bgp allow-ibgp** command with care, because it redistributes both EBGP and IBGP routes that may cause routing loops.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33 and 50 for redistributed routes.

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

```
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **log-peer-change** command to enable the logging of OSPF neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is displayed on the terminal until the feature is disabled.

Examples

Disable the logging of neighbor state changes for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

View

OSPF view

Default Level

2: System level

Parameters

interval: Specifies the minimum LSA repeat arrival interval in milliseconds, in the range 0 to 60000.

Description

Use the **lsa-arrival-interval** command to specify the minimum LSA repeat arrival interval.

Use the **undo lsa-arrival-interval** command to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps protect routers and bandwidth from being over-consumed due to frequent network changes.

It is recommended the interval set with the **lsa-arrival-interval** command is smaller or equal to the initial interval set with the **lsa-generation-interval** command.

Related commands: **lsa-generation-interval**.

Examples

Set the LSA minimum repeat arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

lsa-generation-interval

Syntax

lsa-generation-interval *maximum-interval* [*initial-interval* [*incremental-interval*]]

undo lsa-generation-interval

View

OSPF view

Default Level

2: System level

Parameters

maximum-interval: Maximum LSA generation interval in seconds, in the range 1 to 60.

initial-interval: Minimum LSA generation interval in milliseconds, in the range 10 to 60000. The default is 0.

incremental-interval: LSA generation incremental interval in milliseconds, in the range 10 to 60000. The default is 5000 milliseconds.

Description

Use the **lsa-generation-interval** command to configure the OSPF LSA generation interval.

Use the **undo lsa-generation-interval** command to restore the default.

The LSA generation interval defaults to 5 seconds.

With this command configured, when network changes are not frequent, LSAs are generated at the *initial-interval.* If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

Examples

Configure the maximum LSA generation interval as 2 seconds, minimum interval as 100 milliseconds and incremental interval as 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

lsdb-overflow-limit

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

View

OSPF view

Default Level

2: System level

Parameters

number: Specifies the upper limit of external LSAs in the LSDB, in the range 1 to 1000000.

Description

Use the **lsdb-overflow-limit** command to specify the upper limit of external LSAs in the LSDB.

Use the **undo lsdb-overflow-limit** command to restore the default.

External LSAs in the LSDB are unlimited by default.

Examples

Specify the upper limit of external LSAs as 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing (OSPF view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPF view

Default Level

2: System level

Parameters

maximum: Maximum number of equal cost routes for load balancing, in the range 1 to 4. No load balancing is available when the number is set to 1.

Description

Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes is 4.

Examples

Specify the maximum number of equal cost routes for load balancing as 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

maximum-routes

Syntax

maximum-routes { **external** | **inter** | **intra** } *number*

undo maximum-routes { **external** | **inter** | **intra** }

View

OSPF view

Default Level

2: System level

Parameters

external: Specifies the maximum number of external routes.

inter: Specifies the maximum number of inter-area routes.

intra: Specifies the maximum number of intra-area routes.

number: Maximum route number, in the range 0 to 128000.

Description

Use the **maximum-routes** command to specify the maximum route number of a specified type, inter-area, intra-area or external.

Use the **undo maximum-routes** command to restore the default route maximum value of a specified type.

By default, the maximum route number is 128000.

Examples

Specify the maximum number of intra-area routes as 500.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] maximum-routes intra 500
```

network (OSPF area view)

Syntax

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

View

OSPF area view

Default Level

2: System level

Parameters

ip-address: IP address of a network.

wildcard-mask: Wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Description

Use the **network** command to enable OSPF on the interface attached to the specified network in the area.

Use the **undo network** command to disable OSPF for the interface attached to the specified network in the area.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure one or multiple interfaces in an area to run OSPF. Note that the interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the network segment, the interface cannot run OSPF.

Related commands: **ospf**.

Examples

Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

nssa

Syntax

nssa [**default-route-advertise** | **no-import-route** | **no-summary**] *

undo nssa

View

OSPF area view

Default Level

2: System level

Parameters

default-route-advertise: Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a Type-7 LSA into the NSSA regardless of whether the default route is available. If it is configured on an ASBR, only a default route is available on the ASBR can it generates the default route in a Type-7 LSA into the attached area.

no-import-route: Usable only on an NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing routes in Type7 LSAs into the NSSA area, making sure that routes can be redistributed correctly.

no-summary: Usable only on an NSSA ABR to advertise only a default route in a Type-3 summary LSA into the NSSA area. In this way, all the other summary LSAs are not advertised into the area. Such an area is known as an NSSA totally stub area.

Description

Use the **nssa** command to configure the current area as an NSSA area.

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

By default, no NSSA area is configured.

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost**.

Examples

Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

opaque-capability enable

Syntax

opaque-capability enable

undo opaque-capability

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **opaque-capability enable** command to enable opaque LSA advertisement and reception. With the command configured, the OSPF device can receive and advertise the Type-9, Type-10 and Type-11 opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

The feature is disabled by default.

Examples

Enable advertising and receiving opaque LSAs.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100]opaque-capability enable
```

ospf

Syntax

ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *instance-name*] *

undo ospf [*process-id*]

View

System view

Default Level

2: System level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

router-id: OSPF Router ID, in dotted decimal format.

instance-name: VPN instance name, a string of 1 to 31 characters.

Description

Use the **ospf** command to enable an OSPF process.

Use the **undo ospf** command to disable an OSPF process.

No OSPF process is enabled by default.

You can enable multiple OSPF processes on a router and specify different Router IDs for these processes.

When using OSPF as the IGP for MPLS VPN implementation, you need to bind the OSPF process with a VPN instance.

Enabling OSPF first is required before performing other tasks.

Examples

Enable OSPF process 100 and specify Router ID 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
```

```
[Sysname-ospf-100]
```

ospf authentication-mode

Syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*

undo ospf authentication-mode { **md5** | **hmac-md5** } *key-id*

For simple authentication:

ospf authentication-mode simple [**plain** | **cipher**] *password*

undo ospf authentication-mode simple

View

Interface view

Default Level

2: System level

Parameters

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range 1 to 255.

plain | **cipher**: Plain or cipher password. If **plain** is specified, only plain password is supported and displayed upon displaying the configuration file. If **cipher** is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. If no keyword is specified, the cipher type is the default for the MD5/HMAC-MD5 authentication mode, and the plain type is the default for the simple authentication mode.

password: Password. Simple authentication: For plain type password, a plain password is a string of up to 8 characters; for cipher type password, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type password, a plain password is a string of up to16 characters; for cipher type password, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description

Use the **ospf authentication-mode** command to set the authentication mode and key ID on an interface.

Use the **undo ospf authentication-mode** command to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

This configuration is not supported on the null interface.

Related commands: **authentication-mode**.

Examples

Configure the network 131.119.0.0/16 in Area 1 to support MD5 cipher authentication, and set the interface key ID to 15, authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 cipher abc
```

Configure the network 131.119.0.0/16 in Area 1 to support simple authentication, and set for the interface the authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple cipher abc
```

ospf cost

Syntax

ospf cost *value*

undo ospf cost

View

Interface view

Default Level

2: System level

Parameters

value: OSPF cost, in the range 1 to 65535.

Description

Use the **ospf cost** command to set an OSPF cost for the interface.

Use the **undo ospf cost** command to restore the default.

By default, an OSPF interface calculates its cost with the formula: interface default OSPF cost=100 Mbps/interface bandwidth(Mbps). Default OSPF costs of some interfaces are:

- 1785 for the 56 kbps serial interface

- 1562 for the 64 kbps serial interface
- 48 for the E1 (2.048 Mbps) interface
- 1 for the Ethernet interface

You can use the **ospf cost** command to set an OSPF cost for an interface manually.

Note

This configuration is not supported on the null or loopback interfaces .

Examples

Set the OSPF cost for the interface to 65.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf cost 65
```

ospf dr-priority

Syntax

ospf dr-priority *priority*

undo ospf dr-priority

View

Interface view

Default Level

2: System level

Parameters

priority: DR Priority of the interface, in the range 0 to 255.

Description

Use the **ospf dr-priority** command to set the priority for DR/BDR election on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

By default, the priority is 1.

The bigger the value, the higher the priority.

The DR priority configuration is not supported on the null and loopback interfaces.

Examples

Set the DR priority on the current interface to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf dr-priority 8
```

ospf mib-binding

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

View

System view

Default Level

2: System level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **ospf mib-binding** command to bind an OSPF process to MIB operation.

Use the **undo ospf mib-binding** command to restore the default.

By default, MIB operation is bound to the first enabled OSPF process.

Examples

Bind OSPF process 100 to MIB operation.

```
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

Restore the default, that is, bind the first enabled OSPF process to MIB operation.

```
<Sysname> system-view
[Sysname] undo ospf mib-binding
```

ospf mtu-enable

Syntax

ospf mtu-enable

undo ospf mtu-enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ospf mtu-enable** command to enable an interface to add the real MTU into DD packets.

Use the **undo ospf mtu-enable** command to restore the default.

By default, an interface adds a MTU of 0 into DD packets, that is, no real MTU is added.

Note that:

- After a virtual link is established via a Tunnel, two devices on the link from different vendors may have different MTU values. To make them consistent, set the attached interfaces' default MTU to 0.
- This configuration is not supported on the null interface.

Examples

Enable the interface to add the real MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf mtu-enable
```

ospf network-type

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** | **p2p** }

undo ospf network-type

View

Interface view

Default Level

2: System level

Parameters

broadcast: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

Description

Use the **ospf network-type** command to set the network type for an interface.

Use the **undo ospf network-type** command to restore the default network type for an interface.

By default, the network type of an interface depends on its link layer protocol.

- For Ethernet, and FDDI, the default network type is broadcast.
- For ATM, FR, and X.25, the default network type is NBMA.
- For PPP, LAPB, HDLC, and POS, the default network type is P2P.

Note that:

- If a router on a broadcast network does not support multicast, you can configure the interface's network type as NBMA.
- If any two routers on an NBMA network are directly connected via a virtual link, that is, the network is fully meshed, you can configure the network type as NBMA; otherwise you need to configure it as P2MP for two routers having no direct link to exchange routing information via another router.

- When the network type of an interface is NBMA, you need to use the **peer** command to specify a neighbor.
- If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

Related commands: **ospf dr-priority**.

Note

This command is not supported on the null or loopback interfaces.

Examples

Configure the interface's network type as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf network-type nbma
```

ospf packet-process prioritized-treatment

Syntax

ospf packet-process prioritized-treatment

undo ospf packet-process prioritized-treatment

View

System view

Parameters

None

Description

Use the **ospf packet-process prioritized-treatment** command to enable OSPF to give priority to receiving and processing Hello packets.

Use the **undo ospf packet-process prioritized-treatment** command to restore the default.

By default, this function is not enabled.

Examples

Enable OSPF to give priority to receiving and processing Hello packets.

```
<Sysname> system-view
[Sysname] ospf packet-process prioritized-treatment
```

ospf timer dead

Syntax

ospf timer dead *seconds*

undo ospf timer dead

View

Interface view

Default Level

2: System level

Parameters

seconds: Dead interval in seconds, in the range 1 to 2147483647.

Description

Use the **ospf timer dead** command to set the dead interval.

Use the **undo ospf timer dead** command to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces.

If an interface receives no hello packet from the neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.

This configuration is not supported on the null interface.

Related commands: **ospf timer hello**.

Examples

Configure the dead interval on the current interface as 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer dead 60
```

ospf timer hello

Syntax

ospf timer hello *seconds*

undo ospf timer hello

View

Interface view

Default Level

2: System level

Parameters

seconds: Hello interval in seconds, in the range 1 to 65535.

Description

Use the **ospf timer hello** command to set the hello interval on an interface.

Use the **undo ospf timer hello** command to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces.

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

This configuration is not supported on the null interface.

Related commands: **ospf timer dead**.

Examples

Configure the hello interval on the current interface as 20 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer hello 20
```

ospf timer poll

Syntax

ospf timer poll *seconds*

undo ospf timer poll

View

Interface view

Default Level

2: System level

Parameters

seconds: Poll interval in seconds, in the range 1 to 2147483647.

Description

Use the **ospf timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospf timer poll** command to restore the default value.

By default, the poll interval is 120s.

When an NBMA interface finds its neighbor is down, it will send hello packets at the poll interval.

The poll interval is at least four times the hello interval.

This configuration is not supported on the null interface.

Related commands: **ospf timer hello**.

Examples

Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

ospf timer retransmit

Syntax

ospf timer retransmit *interval*

undo ospf timer retransmit

View

Interface view

Default Level

2: System level

Parameters

interval: LSA retransmission interval in seconds, in the range 1 to 3600.

Description

Use the **ospf timer retransmit** command to set the LSA retransmission interval on an interface.

Use the **undo ospf timer retransmit** command to restore the default.

The interval defaults to 5s.

After sending an LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement within the retransmission interval, it will retransmit the LSA.

The retransmission interval should not be so small to avoid unnecessary retransmissions.

This configuration is not supported on the null interface.

Examples

Set the LSA retransmission interval to 8 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer retransmit 8
```

ospf trans-delay

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

View

Interface view

Default Level

2: System level

Parameters

seconds: LSA transmission delay in seconds, in the range 1 to 3600.

Description

Use the **ospf trans-delay** command to set the LSA transmission delay on an interface.

Use the **undo ospf trans-delay** command to restore the default.

The delay defaults to 1s.

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. It is necessary to add a transmission delay into its age time, which is important for low speed networks.

This configuration is not supported on the null interface.

Examples

Set the LSA transmission delay to 3 seconds on the current interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf trans-delay 3
```

peer

Syntax

peer *ip-address* [**dr-priority** *dr-priority*]

undo peer *ip-address*

View

OSPF view

Default Level

2: System level

Parameters

ip-address: Neighbor IP address.

dr-priority: Neighbor DR priority, in the range 0 to 255.

Description

Use the **peer** command to specify a neighbor, and the DR priority of the neighbor.

Use the **undo peer** command to remove the configuration.

On an Frame Relay network, you can configure mappings to make the network fully meshed (any two routers have a direct link in between), so OSPF can handle DR/BDR election as it does on a broadcast network. However, since routers on the network cannot find neighbors via broadcasting hello packets, you need to specify neighbors and neighbor DR priorities on the routers.

After startup, a router sends a hello packet to neighbors with DR priorities higher than 0. When the DR and BDR are elected, the DR will send hello packets to all neighbors for adjacency establishment.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

Examples

Specify the neighbor 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

preference

Syntax

preference [**ase**] [**route-policy** *route-policy-name*] *value*

undo preference [**ase**]

View

OSPF view

Default Level

2: System level

Parameters

ase: Sets a priority for ASE routes. If the keyword is not specified, using the command sets a priority for OSPF internal routes.

route-policy *route-policy-name*: Applies a route policy to set priorities for specified routes. r*oute-policy-name* is a string of 1 to 19 characters.

value: Priority value, in the range 1 to 255. A smaller value represents a higher priority.

Description

Use the **preference** command to set the priority of OSPF routes.

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

The priority of OSPF internal routes defaults to 10, and the priority of OSPF external routes defaults to 150.

If a route policy is specified, priorities defined by the route policy will apply to matching routes, and the priorities set with the **preference** command apply to OSPF routes not matching the route policy.

A router may run multiple routing protocols. When several routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest priority.

Examples

Set a priority of 200 for OSPF external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference ase 200
```

reset ospf counters

Syntax

reset ospf [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

View

User view

Default Level

2: System level

Parameters

process-id: Clears the statistics information of the specified OSPF process, which is in the range 1 to 65535.

neighbor: Clears neighbor statistics.

interface-type interface-number: Clears the statistics information of the neighbor connected to the specified interface.

router-id: Clears the statistics information of the specified neighbor.

Description

Use the **reset ospf counters** command to clear OSPF statistics information.

Examples

Reset OSPF counters.

```
<Sysname> reset ospf counters
```

reset ospf process

Syntax

reset ospf [*process-id*] **process** [**graceful-restart**]

View

User view

Default Level

2: System level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

graceful-restart: Starts GR for the OSPF process.

Description

Use the **reset ospf process** command to reset all OSPF processes or a specified process.

Using the **reset ospf process** command will:

- Clear all invalid LSAs without waiting for their timeouts;
- Make a newly configured Router ID take effect;
- Start a new round of DR/BDR election;
- Not remove any previous OSPF configurations.

The system prompts whether to reset OSPF process upon execution of this command.

Examples

Reset all OSPF processes.

```
<Sysname> reset ospf process
```

reset ospf redistribution

Syntax

reset ospf [*process-id*] **redistribution**

View

User view

Default Level

2: System level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

Description

Use the **reset ospf redistribution** command to restart route redistribution. If no process ID is specified, using the command restarts route redistribution for all OSPF processes.

Examples

Restart route redistribution.

```
<Sysname> reset ospf redistribution
```

rfc1583 compatible

Syntax

rfc1583 compatible

undo rfc1583 compatible

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **rfc1583 compatible** command to make routing rules defined in RFC1583 compatible.

Use the **undo rfc1583 compatible** command to disable the function.

By default, RFC1583 routing rules are compatible.

RFC1583 and RFC2328 have different routing rules on selecting the best route when multiple AS external LSAs describe routes to the same destination. Using this command can make them compatible.

Examples

Disable making RFC1583 routing rules compatible.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo rfc1583 compatible
```

silent-interface (OSPF view)

Syntax

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View

OSPF view

Default Level

2: System level

Parameters

all: Disables all interfaces from sending OSPF packets.

interface-type interface-number: Disables the specified interface from sending OSPF packets

Description

Use the **silent-interface** command to disable an interface or all interfaces from sending OSPF packets.

Use the **undo silent-interface** command to restore the default.

By default, an interface sends OSPF packets.

A disabled interface is a passive interface, which cannot send any hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from sending OSPF packets.

Examples

Disable an interface from sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface vlan-interface 10
```

snmp-agent trap enable ospf

Syntax

snmp-agent trap enable ospf [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa**

| **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

undo snmp-agent trap enable ospf [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

View

System view

Default Level

3: Manage level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

ifauthfail: Interface authentication failure information.

ifcfgerror: Interface configuration error information.

ifrxbadpkt: Information about error packets received.

ifstatechange: Interface state change information.

iftxretransmit: Packet receiving and forwarding information.

lsdbapproachoverflow: Information about cases approaching LSDB overflow.

lsdboverflow: LSDB overflow information.

maxagelsa: LSA max age information.

nbrstatechange: Neighbor state change information.

originatelsa: Information about LSAs originated locally.

vifauthfail: Virtual interface authentication failure information.

vifcfgerror: Virtual interface configuration error information.

virifauthfail: Virtual interface authentication failure information.

virifrxbadpkt: Information about error packets received by virtual interfaces.

virifstatechange: Virtual interface state change information.

viriftxretransmit: Virtual interface packet retransmission information.

virnbrstatechange: Virtual interface neighbor state change information.

Description

Use the **snmp-agent trap enable ospf** command to enable the sending of SNMP traps for a specified OSPF process. If no process is specified, the feature is enabled for all processes.

Use the **undo snmp-agent trap enable ospf** command to disable the feature.

By default, this feature is enabled.

Refer to *SNMP Commands* in the *System Volume* for related information.

Examples

Enable the sending of SNMP traps for OSPF process 1.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ospf 1
```

spf-schedule-interval

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

View

OSPF view

Default Level

2: System level

Parameters

maximum-interval: Maximum OSPF route calculation interval in seconds, in the range 1 to 60.

minimum-interval: Minimum OSPF route calculation interval in milliseconds, in the range 10 to 60000, which defaults to 0.

incremental-interval: Incremental value in milliseconds, in the range 10 to 60000, which defaults to 5000.

Description

Use the **spf-schedule-interval** command to set the OSPF SPF calculation interval.

Use the **undo spf-schedule-interval** command to restore the default.

The interval defaults to 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, and uses it to determine the next hop to a destination. Through adjusting the SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval.* If network changes become frequent, the SPF calculation interval is incremented by the *incremental-interval* each time a calculation happens, up to the *maximum-interval*.

Examples

Configure the SPF calculation maximum interval as 10 seconds, minimum interval as 500 milliseconds and incremental interval as 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 200
```

stub (OSPF area view)

Syntax

stub [**no-summary**]

undo stub

View

OSPF area view

Default Level

2: System level

Parameters

no-summary: Usable only on a stub ABR. With it configured, the ABR advertises only a default route in a Summary LSA into the stub area (such a stub area is known as a totally stub area).

Description

Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

No area is stub area by default.

Note that, to concel the **no-summary** configuration on the ABR, simply execute the **stub** command again to overwrite it.

To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost**.

Examples

Configure Area1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

stub-router

Syntax

stub-router

undo stub-router

View

OSPF view

Default Level

2: System level

Parameters

None

Description

Use the **stub-router** command to configure the router as a stub router.

Use the **undo stub-router** command to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link; in such cases, a maximum cost value of 65535 is used. Thus, other neighbors find the links to the stub router have such big costs, they will not send packets to the stub router for forwarding as long as there is a route with a smaller cost.

Examples

Configure a stub router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

transmit-pacing

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

View

OSPF view

Default Level

2: System level

Parameters

interval: Interval at which an interface sends LSU packets, in milliseconds. Its value is in the range 10 to 1000. If the router has a number of OSPF interfaces, you are recommended to increase this interval to reduce the total numbers of LSU packets sent by the router every second.

count: Maximum number of LSU packets sent by an interface at each interval. It is in the range 1 to 200. If the router has a number of OSPF interfaces, you are recommended to decrease this interval to reduce the total numbers of LSU packets sent by the router every second.

Description

Use the **transmit-pacing** command to configure the maximum number of LSU packets that can be sent every the specified interval.

Use the **undo transmit-pacing** command to restore the default.

By default, an OSPF interface sends up to three LSU packets every 20 milliseconds.

Examples

Configure all the interfaces under OSPF process 1 to send up to 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

vlink-peer (OSPF area view)

Syntax

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**plain** | **cipher**] *password* | { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | [**simple** | { **md5** | **hmac-md5** } *key-id*]] *

View

OSPF area view

Default Level

2: System level

Parameters

router-id: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds, in the range 1 to 8192. The default is 10. It must be identical to the hello interval on its virtual link neighbor.

retransmit *seconds*: Retransmission interval in seconds, in the range 1 to 3600, which defaults to 5.

trans-delay *seconds*: Transmission delay interval in seconds, in the range 1 to 3600, which defaults to 1.

dead *seconds*: Dead interval in seconds, in the range 1 to 32768, which defaults to 40 and is identical to the value on its virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range 1 to 255.

plain | **cipher**: Plain or cipher type. If plain is specified, only plain password is supported and displayed upon displaying the configuration file. If cipher is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. By default, MD5 and HMAC-MD5 support cipher password, and simple authentication supports plain password.

password: Plain or cipher password. Simple authentication: For plain type, a plain password is a string of up to 8 characters. For cipher type, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type, a plain password is a string of up to16 characters. For cipher type, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description

Use the **vlink-peer** command to configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

As defined in RFC2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Considerations on parameters:

- The smaller the hello interval is, the faster the network converges and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A big value is appropriate for a low speed link.
- You need to specify an appropriate transmission delay with the **trans-delay** keyword.

The authentication mode at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes (MD5 or Simple) are independent, and you can specify neither of them.

Related commands: **authentication-mode**, **display ospf**.

Examples

Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

Table of Contents

1 IS-IS Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

IS-IS Configuration Commands

area-authentication-mode

Syntax

area-authentication-mode { **simple** | **md5** } *password* [**ip** | **osi**]

undo area-authentication-mode

View

IS-IS view

Default Level

2: System level

Parameters

simple: Specifies the simple authentication mode.

md5: Specifies the MD5 authentication mode.

password: Password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plaintext password can be a string of up to 16 characters, such as **user918**. A cipher password must be a ciphertext string of 24 characters, such as **(TT8F]Y\5SQ=^Q`MAF4<1!!**.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

Note

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description

Use the **area-authentication-mode** command to specify the area authentication mode and a password.

Use the **undo area-authentication-mode** command to restore the default.

No area authentication is configured by default.

The password in the specified mode is inserted into all outgoing Level-1 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-1 packets.

With area authentication configured, IS-IS discards incoming routes from untrusted routers.

Note that:

- Routers in a common area must have the same authentication mode and password.
- If neither **ip** nor **osi** is specified, OSI related fields are checked.

Related commands: **reset isis all**, **domain-authentication-mode**, **isis authentication-mode**

Examples

Set the area authentication password to ivg, and the authentication mode to simple.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] area-authentication-mode simple ivg
```

auto-cost enable

Syntax

auto-cost enable

undo auto-cost enable

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **auto-cost enable** command to enable automatic link cost calculation.

Use the **undo auto-cost enable** command to disable the function.

This function is disabled by default.

After automatic link cost calculation is enabled, the link cost is automatically calculated based on the bandwidth reference value of an interface. When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the formula: Cost = (reference bandwidth value/link bandwidth) × 10.

Related commands: **bandwidth-reference**, **cost-style**.

Examples

Enable automatic link cost calculation.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] auto-cost enable
```

bandwidth-reference (IS-IS view)

Syntax

bandwidth-reference *value*

undo bandwidth-reference

View

IS-IS view

Default Level

2: System level

Parameters

value: Bandwidth reference value in Mbps, ranging from 1 to 2147483648.

Description

Use the **bandwidth-reference** command to set the bandwidth reference value for automatic link cost calculation.

Use the **undo bandwidth-reference** command to restore the default.

By default, the bandwidth reference value is 100 Mbps.

Related commands: **auto-cost enable**.

Examples

Configure the bandwidth reference of IS-IS process 1 as 200 Mbps.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] bandwidth-reference 200
```

circuit-cost

Syntax

circuit-cost *value* [**level-1** | **level-2**]

undo circuit-cost [**level-1** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

value: Link cost value. The value range varies with cost styles.

- For styles **narrow, narrow-compatible** and **compatible**, the cost value ranges from 0 to 63.
- For styles **wide** and **wide-compatible**, the cost value ranges from 0 to 16777215.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Description

Use the **circuit-cost** command to set a global IS-IS link cost.

Use the **undo circuit-cost** command to restore the default.

By default, no global link cost is configured.

If no level is specified, the specified cost applies to both Level-1 and Level-2.

Related commands: **isis cost**, **cost-style**.

Examples

Set the global Level-1 link cost of IS-IS process 1 to 11.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] circuit-cost 11 level-1
```

cost-style

Syntax

cost-style { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

View

IS-IS view

Default Level

2: System level

Parameters

narrow: Receives and sends only narrow cost style packets (The narrow cost ranges from 0 to 63).

wide: Receives and sends only wide cost style packets (The wide cost ranges from 0 to 16777215).

compatible: Receives and sends both wide and narrow cost style packets.

narrow-compatible: Receives both narrow and wide cost style packets, but sends only narrow cost style packets.

wide-compatible: Receives both narrow and wide cost style packets, but sends only wide cost style packets.

relax-spf-limit: Allows receiving routes with a cost greater than 1023. If this keyword is not specified, any route with a cost bigger than 1023 will be discarded. This keyword is only available when **compatible** or **narrow-compatible** is included.

Description

Use the **cost-style** command to set a cost style.

Use the **undo cost-style** command to restore the default.

Only narrow cost style packets can be received and sent by default.

Related commands: **isis cost**, **circuit-cost**.

Examples

Configure the router to send only narrow cost style packets, but receive both narrow and wide cost style packets.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] cost-style narrow-compatible
```

default-route-advertise (IS-IS view)

Syntax

default-route-advertise [**route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo default-route-advertise [**route-policy** *route-policy-name*]

View

IS-IS view

Default Level

2: System level

Parameters

route-policy-name: Specifies the name of a routing policy, a string of 1 to 19 characters.

level-1: Advertises a Level-1 default route.

level-2: Advertises a Level-2 default route.

level-1-2: Advertises both Level-1 and Level-2 default routes.

Description

Use the **default-route-advertise** command to advertise a default route of 0.0.0.0/0.

Use the **undo default-route-advertise** command to disable default route advertisement.

Default route advertisement is disabled by default.

Note that:

- If no level is specified, a Level-2 default route is advertised.
- The Level-1 default route is advertised to other routers in the same area, while the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.
- Using the **apply isis level-1** command in routing policy view will generate a default route in a Level-1 LSP. Using the **apply isis level-2** command in routing policy view will generate a default route in a Level-2 LSP. Using the **apply isis level-1-2** command in routing policy view will generate a default route in a Level-1 LSP and Level-2 LSP respectively.

Examples

Advertise a Level-2 default route.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] default-route-advertise
```

display isis brief

Syntax

display isis brief [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays IS-IS brief configuration information for the IS-IS process. The process ID is in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Displays IS-IS brief configuration information for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

Description

Use the **display isis brief** command to view IS-IS brief configuration information.

Examples

Display IS-IS brief configuration information.

```
<Sysname> display isis brief

                  ISIS (1) Protocol Brief Information :


 network-entity:
     10.0000.0000.0001.00
 is-level :level-1-2
 cost-style:  narrow
 preference :  15
 Lsp-length receive :  1497
 Lsp-length originate :  level-1 1497
                         level-2 1497
maximum imported routes number     : 10000
 Timers:
     lsp-max-age:  1200
     lsp-refresh:  900
     Interval between SPFs:  10
```

Table 1-1 display isis brief command output description

Field		Description
network-entity		Network entity name
is-level		IS-IS Routing level
cost-style		Cost style
preference		Preference
Lsp-length receive		Maximum LSP that can be received
Lsp-length originate		Maximum LSP that can be generated
maximum imported routes number		Maximum number of redistributed Level-1/Level-2 IPv4 routes
Timers	lsp-max-age	Maximum life period of LSP
	lsp-refresh	Refresh interval of LSP
	Interval between SPFs	Interval between SPF calculations

display isis debug-switches

Syntax

display isis debug-switches { *process-id* | **vpn-instance** *vpn-instance-name* }

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays the IS-IS debugging switch state for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the IS-IS debugging switch state for the VPN instance. The name is a string of 1 to 31 characters.

Description

Use the **display isis debug-switches** command to display IS-IS debugging switch state.

Examples

Display the debugging switch state of IS-IS process 1.

```
<Sysname> display isis debug-switches 1
IS-IS - Debug settings.
        IS-IS SPF Triggering Events debugging is on
```

display isis graceful-restart status

Syntax

display isis graceful-restart status [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

level-1: Displays the IS-IS Level-1 Graceful Restart state.

level-2: Displays the IS-IS Level-2 Graceful Restart state.

process-id: IS-IS Process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

Description

Use the **display isis graceful-restart status** command to display IS-IS Graceful Restart status.

Examples

Display IS-IS Graceful Restart status.

```
<Sysname> display isis graceful-restart status
                Restart information for IS-IS(1)
--------------------------------------------------------------------------
IS-IS(1) Level-1 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  Number of LSPs Awaited: 3
  T3 Timer Status:
    Remaining Time: 140
  T2 Timer Status:
    Remaining Time: 59

IS-IS(1) Level-2 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  Number of LSPs Awaited: 3
  T3 Timer Status:
    Remaining Time: 140
  T2 Timer Status:
Remaining Time: 59
```

Table 1-2 display isis graceful-restart status command output description

Field	Description
Restart Interval	Graceful Restart interval
SA Bit Supported	The SA bit is set
Total Number of Interfaces = 1	The current IS-IS interface number
Restart Status:	Graceful Restart status
Number of LSPs Awaited	Number of LSPs not obtained by the GR restarter from GR helpers during LSDB synchronization
T3 Timer Status	Remaining time of T3 timer
T2 Timer Status:	Remaining time of T2 Timer

display isis interface

Syntax

display isis interface [**statistics** | [*interface-type interface-number*] [**verbose**]] [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

statistics: Displays IS-IS interface statistics information.

interface-type interface-number: IS-IS interface whose statistics information is to be displayed.

verbose: Displays detailed IS-IS interface information.

process-id: Displays the IS-IS interface information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the IS-IS interface information of the VPN instance. The name is a string of 1 to 31 characters.

Description

Use the **display isis interface** command to display IS-IS interface information.

Examples

Display brief IS-IS interface information.

```
<Sysname> display isis interface
                      Interface information for ISIS(1)
                      --------------------------------
Interface: Vlan-interface1
Id      IPV4.State        IPV6.State     MTU    Type    DIS
001       Up                Down       1497    L1/L2   No/No
```

Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose

                      Interface information for ISIS(1)
                      --------------------------------

  Interface:  Vlan-interface999
  Id      IPV4.State           IPV6.State        MTU  Type  DIS
  001          Up                   Down          1497 L1/L2 No/No
  SNPA Address               : 000f-e237-c6e0
  IP Address                 : 192.168.1.48
  Secondary IP Address(es)   :
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value           :  L1    10  L2    10
  Hello Timer Value          :  L1    10  L2    10
  Hello Multiplier Value     :  L1     3  L2     3
  Lsp Timer Value            :  L12   33
  Cost                       :  L1    10  L2    10
  Priority                   :  L1    64  L2    64
  Retransmit Timer Value     :  L12    5
  BFD                        :  Disabled
  MPLS TE Status             :  OFF
  INTF L1 TE Status          :  OFF
  INTF L2 TE Status          :  OFF
  TE Cost                    :  0
  TE Admin Group             :  0
  TE Max Bandwidth           :  0
  TE Max Res Bandwidth       :  0
```

Displays detailed information of the specified IS-IS interface.

```
<Sysname> display isis interface Tunnel 1 verbose

                      Interface information for ISIS(1)
                      --------------------------------

  Interface:  Tunnel1
  Id      IPv4.State           IPv6.State        MTU  Type  DIS
  005          Up                   Down          16384L1/L2 --
  SNPA Address               : 0000-0000-0000
  IP Address                 : 10.1.1.4
  Secondary IP Address(es)   :
  IPv6 Link Local Address    :
  IPv6 Global Address(es)    :
  Csnp Timer Value           :  L1    10  L2    10
  Hello Timer Value          :        10
  Hello Multiplier Value     :         3
  Cost                       :  L1    10  L2    10
```

```
Priority                    :  L1    64  L2    64
Retransmit Timer Value      :  L12    5
Retransmit-Throttle Timer   :  L12   33
BFD                         :  Disabled
Tunnel L1 State             :  OFF
Tunnel L2 State             :  ON
Tunnel Type                 :  AA
Tunnel Metric               :  0
Destination Router ID       :  5.5.5.5
```

Table 1-3 display isis interface command output description

Field	Description
Interface	Interface type and number
Id	Circuit ID
IPV4.State	IPv4 state
IPV6.State	IPv6 state
MTU	Interface MTU
Type	Interface link adjacency type
DIS	Whether the interface is elected as the DIS or not
SNPA Address	Subnet access point address
IP Address	Primary IP address
Secondary IP Address(es)	Secondary IP addresses
IPV6 Link Local Address	IPv6 link local address
IPV6 Global Address(es)	IPv6 global address
Csnp Timer Value	Interval for sending CSNP packets
Hello Timer Value	Interval for sending Hello packets
Hello Multiplier Value	Number of invalid Hello packets
Lsp Timer Value	Minimum interval for sending LSP packets
Cost	Cost of the interface
Priority	DIS priority
Retransmit Timer Value	LSP retransmission interval over the point-to-point link
BFD	Whether BFD is enabled on the interface
MPLS TE Status	Whether MPLS TE is enabled on the interface
INTF L1 TE Status	Whether level-1 MPLS TE is enabled on the interface
INTF L2 TE Status	Whether level-2 MPLS TE is enabled on the interface
TE Cost	MPLS TE cost configured on the interface
TE Admin Group	TE link administration group
TE Max Bandwidth	TE link maximum bandwidth
TE Max Res Bandwidth	TE link maximum reserved bandwidth
Tunnel L1 State	IS-IS TE tunnel level-1 state

Field	Description
Tunnel L2 State	IS-IS TE tunnel level-2 state
Tunnel Type	Tunnel type
Tunnel Metric	IGP metric of the TE tunnel
Destination Router ID	Destination address of TE tunnel inteface

Display IS-IS interface statistics information.

```
<sysname> display isis interface statistics
                  Interface Statistics information for ISIS(1)
                  ----------------------------------------
  Type            IPv4 Up/Down           IPv6 Up/Down
  LAN                   0/1                    -/-
  P2P                   4/0                    -/-
```

Table 1-4 display isis interface statistics command output description

Field	Description
Type	Network type of the interface: • LAN for broadcast network. • P2P for point-to-point network.
IPv4 UP	Number of IS-IS interfaces in up state
IPv4 DOWN	Number of IS-IS interfaces in down state
IPv6 UP	Number of IS-ISv6 interfaces in up state. A value of "-" means IPv6 is not enabled.
IPv6 DOWN	Number of IS-ISv6 interfaces in down state. A value of "-" means IPv6 is not enabled.

display isis license

Syntax

display isis license

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display isis license** command to display the information of the IS-IS license.

Examples

Display the information of the IS-IS license.

```
<Sysname> display isis license

                      ISIS Shell License Values
                      _________________________

 Feature Name         Active     Controllable
 ISIS Protocol        YES         NO
 IPV6                 YES         NO
 RESTART              YES         NO
 TE                   NO         NO
 MI                   YES         NO

 Resource Name             MinVal     MaxVal     CurrVal    Controllable
 Max Processes Resource    1          1024       500        0
 Max Paths Resource        1          6          3          0
 Max IPv4 Rt Resource      400000     400000     400000     0
 Max IPv6 Rt Resource      400000     400000     400000     0

                      ISIS Core License Values
                      ________________________

 Feature Name         Active
 ISIS Protocol        YES
 IPV6                 YES
 RESTART              YES
 TE                   NO
 MI                   YES

 Resource Name             Current Value
 Max Processes Resource    500
 Max Paths Resource        3
 Max IPv4 Rt Resource      400000
 Max IPv6 Rt Resource      400000
```

Table 1-5 display isis license command output description

Field	Description
ISIS Shell License Values	License values of IS-IS shell
Feature Name	Feature name
Active	Whether the state is active.
Controllable	Whether support reading configuration through License file.
ISIS Protocol	IS-IS Protocol
IPV6	Whether IPv6 is active or not.
RESTART	Graceful Restart (GR)
TE	Traffic Engineering
MI	Multi-instance

Field	Description
Resource Name	Resource name
MinVal	Minimum value
MaxVal	Maximum value
CurrVal	Current value
ISIS Core License Values	License values of IS-IS Core
Max Processes Resource	Maximum number of processes supported
Max Paths Resource	Maximum equal cost paths
Max IPv4 Rt Resource	Maximum IPv4 routes supported
Max IPv6 Rt Resource	Maximum IPv6 routes supported

display isis lsdb

Syntax

display isis lsdb [[**l1** | **l2** | **level-1** | **level-2**] | [**lsp-id** *LSPID* | **lsp-name** *lspname*] | **local** | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

l1, **level-1**: Displays the level-1 LSDB.

l2, **level-2**: Displays the level-2 LSDB.

LSPID: LSP ID, in the form of sysID. Pseudo ID-fragment num, where sysID represents the originating node or pseudo node.

lspname: LSP name, in the form of Symbolic name.[Pseudo ID]-fragment num.

local: Displays LSP information generated locally.

verbose: Displays LSDB detailed information.

process-id: Displays the LSDB of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the LSDB of the VPN instance. The VPN instance name is a string of 1 to 31 characters.

Description

Use the **display isis lsdb** command to display IS-IS link state database.

If no level is specified, both Level-1 and Level-2 link state databases are displayed.

Examples

Display brief Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------

1111.1111.1111.00-00  0x00000004   0xa76         563           68      0/0/0
1111.1111.1112.00-00* 0x00000006   0x498d        578           84      0/0/0
1111.1111.1112.01-00* 0x00000001   0x4c0e        556           55      0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Display detailed Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1 verbose

                       Database information for ISIS(1)
                       --------------------------------

                         Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------

1111.1111.1111.00-00  0x00000005   0x877         1090          68      0/0/0
 SOURCE       1111.1111.1111.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    3.1.1.2
 NBR  ID      1111.1111.1112.01  COST: 10
 IP-Internal  3.1.1.0        255.255.255.0    COST: 10

1111.1111.1112.00-00* 0x00000007   0x478e        1120          84      0/0/0
 SOURCE       1111.1111.1112.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    3.1.1.1
 INTF ADDR    2.1.2.2
 NBR  ID      1111.1111.1112.01  COST: 10
 IP-Internal  3.1.1.0        255.255.255.0    COST: 10
 IP-Internal  2.1.2.0        255.255.255.0    COST: 10

1111.1111.1112.01-00* 0x00000002   0x4a0f        1118          55      0/0/0
 SOURCE       1111.1111.1112.01
 NLPID        IPV4
 NBR  ID      1111.1111.1112.00  COST: 0
 NBR  ID      1111.1111.1111.00  COST: 0
```

```
*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Table 1-6 display isis lsdb command output description

Field	Description
LSPID	Link state packet ID
Seq Num	LSP sequence number
Checksum	LSP checksum
Holdtime	LSP lifetime which decreases as time elapses
Length	LSP length
ATT/P/OL	Attach bit (ATT) Partition bit (P) Overload bit (OL) 1 means the bit is set and 0 means the bit is not set.
SOURCE	System ID of the originating router
NLPID	Network layer protocol the originating router runs
AREA ADDR	Area address of the originating router
INTF ADDR	IP address of the originating router's IS-IS interface
INTF ADDR V6	IPv6 address of the originating router's IS-ISv6 interface
NBR ID	Neighbor ID of the originating router
IP-Internal	Internal IP address and mask of the originating router
IP-External	External IP address and mask of the originating router
IP-Extended	Extended IP address and mask of the originating router
COST	Cost
HOST NAME	Dynamic host name of the originating router
ORG ID	Original system ID of the virtual system ID of the originating router
Auth	Authentication information of the originating router
IPV6	Internal IPv6 address and prefix of the originating router
IPV6-Ext	External IPv6 address and prefix of the originating router

display isis mesh-group

Syntax

display isis mesh-group [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays IS-IS mesh-group configuration information for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays IS-IS mesh-group configuration information for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

Description

Use the **display isis mesh-group** command to display IS-IS mesh-group configuration information.

Examples

Configure VLAN-interface 10 and VLAN-interface 20 to belong to mesh-group 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis mesh-group 100
[Sysname-Vlan-interface10] interface vlan-interface 20
[Sysname-Vlan-interface20] isis mesh-group 100
```

Display the configuration information of IS-IS mesh-group.

```
[Sysname-Vlan-interface20] display isis mesh-group

                    Mesh Group information for ISIS(1)
                    ----------------------------------
 Interface          Status
 Vlan10              100
 Vlan20              100
```

Table 1-7 display isis mesh-group command output description

Field	Description
Interface	Interface name
Status	Mesh-group the interface belongs to

display isis name-table

Syntax

display isis name-table [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays the host name-to-system ID mapping table for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the host name-to-system ID mapping table for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

Description

Use the **display isis name-table** command to display the host name-to-system ID mapping table.

Examples

Configure a name for the local IS system.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

Configure a static mapping for the remote IS system (system ID 0000.0000.0041, host name RUTB).

```
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

Display the IS-IS host name-to-system ID mapping table.

```
[Sysname-isis-1] display isis name-table
              Name table information for ISIS(1)
-------------------------------------------------------------
System ID            Hostname                          Type
6789.0000.0001       RUTA                              DYNAMIC
0000.0000.0041       RUTB                              STATIC
```

Table 1-8 display isis name-table command output description

Field	Description
System ID	System ID
Hostname	Hostname name
Type	Mapping type (static or dynamic)

display isis peer

Syntax

display isis peer [**verbose | statistics**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed IS-IS neighbor information. Without the keyword, the command displays brief IS-IS neighbor information.

statistics: Displays IS-IS neighbor statistics information.

process-id: Displays the IS-IS neighbor information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the IS-IS neighbor information of the VPN instance. The *vpn-instance-name* is a string of 1 to 31 characters.

Description

Use the **display isis peer** command to display IS-IS neighbor information.

Examples

Display brief IS-IS neighbor information.

```
<Sysname> display isis peer

                         Peer information for ISIS(1)
                         ----------------------------

  System Id: 1111.1111.1111
  Interface: Vlan-interface1           Circuit Id: 1111.1111.1112.01
  State: Up     HoldTime: 23s        Type: L1(L1L2)     PRI: 64

  System Id: 1111.1111.1111
  Interface: Vlan-interface1           Circuit Id: 1111.1111.1112.01
  State: Up     HoldTime: 23s        Type: L2(L1L2)     PRI: 64
```

Display detailed IS-IS neighbor information.

```
<Sysname>display isis peer verbose

                         Peer information for ISIS(1)
                         ----------------------------

  System Id: 1111.1111.1111
  Interface: Vlan-interface1           Circuit Id: 1111.1111.1112.01
  State: Up     HoldTime: 27s        Type: L1(L1L2)     PRI: 64
  Area Address(es):10
  Peer IP Address(es): 3.1.1.2
  Uptime: 00:38:15
  Adj Protocol:  IPV4


  System Id: 1111.1111.1111
  Interface: Vlan-interface1           Circuit Id: 1111.1111.1112.01
  State: Up     HoldTime: 28s        Type: L2(L1L2)     PRI: 64
  Area Address(es):10
  Peer IP Address(es): 3.1.1.2
  Uptime: 00:38:15
  Adj Protocol:  IPV4
```

Table 1-9 display isis peer command output description

Field	Description
System Id	System ID of the neighbor
Interface	Interface connecting to the neighbor
Circuit Id	Circuit ID
State	Circuit state
HoldTime	Holdtime Within the holdtime if no hellos are received from the neighbor, the neighbor is considered down. If a hello is received, the holdtime is reset to the initial value.
Type	Circuit type L1 means the circuit type is Level-1 and the neighbor is a Level-1 router. L2 means the circuit type is Level-2 and the neighbor is a Level-2 router. L1(L1L2) means the circuit type is Level-1 and the neighbor is a Level-1-2 router. L2(L1L2) means the circuit type is Level-2 and the neighbor is a Level-1-2 router.
PRI	DIS priority of the neighbor
Area Address(es)	The neighbor's area address
Peer IP Address(es)	IP address of the neighbor
Uptime	Time that elapsed since the neighbor relationship was formed.
Adj Protocol	Adjacency protocol

Display IS-IS neighbor statistics information.

```
<Sysname> display isis peer statistics

                  Peer Statistics information for ISIS(1)
                  ---------------------------------------
 Type             IPv4 Up/Init             IPv6 Up/Init
 LAN Level-1            0/0                      0/0
 LAN Level-2            0/0                      0/0
 P2P                    3/0                      0/0
```

Table 1-10 display isis peer statistics command output description

Field	Description
Type	Neighbor type: • LAN Level-1: Number of Level-1 neighbors whose network type is broadcast. • LAN Level-2: Number of Level-2 neighbors whose network type is broadcast. • P2P: Number of neighbors whose network type is P2P.
IPv4 Up	Number of IPv4 neighbors in up state
IPv4 Init	Number of IPv4 neighbors in init state
IPv6 Up	Number of IPv6 neighbors in up state
IPv6 Init	Number of IPv6 neighbors in init state

display isis route

Syntax

display isis route [**ipv4**] [[**level-1** | **level-2**] | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv4: Displays IS-IS IPv4 routing information (the default).

verbose: Displays detailed IS-IS IPv4 routing information.

process-id: Displays the IS-IS IPv4 routing information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays the IS-IS IPv4 routing information of the VPN instance. The *vpn-instance-name* is a string of 1 to 31 characters.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.

Description

Use the **display isis route** command to display IS-IS IPv4 routing information.

If no level is specified, both Level-1 and Level-2 routing information will be displayed.

Examples

Display IS-IS IPv4 routing information.

```
<Sysname> display isis route 1

                        Route information for ISIS(1)
                        -----------------------------

                    ISIS(1) IPv4 Level-1 Forwarding Table
                    -------------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 1.1.0.0/16           20         NULL    Vlan1        1.2.1.1         R/L/-
 1.2.0.0/16           10         NULL    Vlan1        Direct          D/L/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set


                    ISIS(1) IPv4 Level-2 Forwarding Table
```

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

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 1.1.0.0/16           20         NULL
 1.2.0.0/16            10         NULL    Vlan1        Direct          D/L/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 1-11 display isis route command output description

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2
IPv4 Destination	IPv4 destination address
IntCost	Interior routing cost
ExtCost	Exterior routing cost
ExitInterface	Exit interface
NextHop	Next hop
Flags	Routing state flag D: Direct route. R: The route has been added into the routing table. L: The route has been advertised in an LSP. U: A route's penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

Display detailed IS-IS IPv4 routing information.

```
<Sysname>display isis route verbose
                        Route information for ISIS(1)
                        ----------------------------

                    ISIS(1) IPv4 Level-1 Forwarding Table
                    -------------------------------------

 IPV4 Dest  : 1.1.0.0/16         Int. Cost : 20             Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 2              Flag      : R/L/-
 NextHop    :                    Interface :                ExitIndex :
    1.2.1.1                           Vlan1                  0x00000008

 IPV4 Dest  : 1.2.0.0/16         Int. Cost : 10             Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 2              Flag      : D/L/-
 NextHop    :                    Interface :                ExitIndex :
    Direct                            Vlan1                  0x00000000
```

```
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set


                    ISIS(1) IPv4 Level-2 Forwarding Table
                    -------------------------------------

IPV4 Dest   : 1.1.0.0/16        Int. Cost : 20             Ext. Cost : NULL
Admin Tag   : -                 Src Count : 2              Flag      : -/-/-

IPV4 Dest   : 1.2.0.0/16        Int. Cost : 10             Ext. Cost : NULL
Admin Tag   : -                 Src Count : 3              Flag      : D/L/-
NextHop     :                   Interface :                ExitIndex :
   Direct                             Vlan1                  0x00000000

     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 1-12 display isis route verbose command output description

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2
IPV4 Dest	IPv4 destination
Int. Cost	Internal route cost
Ext. Cost	External route cost
Admin Tag	Tag
Src Count	Count of advertising sources
Flag	Route state flag R: Indicates the route have been installed into the routing table. L: The route has been flooded in an LSP. U: Route leaking flag. If it is UP, routes from L2 to L1 cannot be advertised back to L2.
Next Hop	Next hop
Interface	Outgoing interface
ExitIndex	Index of the outgoing interface

display isis spf-log

Syntax

display isis spf-log [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays IS-IS SPF log information for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays IS-IS SPF log information for the VPN instance. The name is a string of 1 to 31 characters.

Description

Use the **display isis spf-log** command to display IS-IS SPF log information.

Examples

Display IS-IS SPF log information.

```
<Sysname> display isis spf-log
                       SPF Log information for ISIS(1)
                       ------------------------------
   Level    Trig.Event                      No.Nodes  Duration   StartTime
   L2       IS_SPFTRIG_PERIODIC             2         0          13:3:24
   L1       IS_SPFTRIG_PERIODIC             2         0          13:18:8
   L2       IS_SPFTRIG_PERIODIC             2         0          13:18:8
   L1       IS_SPFTRIG_PERIODIC             2         0          13:32:28
   L2       IS_SPFTRIG_PERIODIC             2         0          13:32:28
   L1       IS_SPFTRIG_PERIODIC             2         0          13:44:0
   L2       IS_SPFTRIG_PERIODIC             2         0          13:44:0
   L1       IS_SPFTRIG_PERIODIC             2         0          13:55:43
-->L2       IS_SPFTRIG_PERIODIC             2         0          13:55:43
   L1       IS_SPFTRIG_PERIODIC             2         0          11:54:12
   L2       IS_SPFTRIG_PERIODIC             2         0          11:54:12
   L1       IS_SPFTRIG_PERIODIC             2         0          12:7:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:7:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:21:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:21:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:35:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:35:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:49:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:49:24
   L1       IS_SPFTRIG_PERIODIC             2         0          13:3:24
```

Table 1-13 display isis spf-log command output description

Field	Description
SPF Log information for ISIS(1)	SPF log information for IS-IS process 1
Level	SPF calculation level
Trig.Event	SPF triggered event
No.Nodes	Number of SPF calculation nodes

Field	Description
Duration	SPF calculation duration
StartTime	SPF calculation start time

display isis statistics

Syntax

display isis statistics [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

level-1: Displays IS-IS Level-1 statistics.

level-2: Displays IS-IS Level-2 statistics.

level-1-2: Displays IS-IS Level-1-2 statistics.

process-id: Displays IS-IS statistics for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance-name: Displays IS-IS statistics for the VPN instance. The name is a string of 1 to 31 characters.

Description

Use the **display isis statistics** command to display IS-IS statistics.

Examples

Display IS-IS statistics.

```
<Sysname> display isis statistics

                      Statistics information for ISIS(1)
                      ----------------------------------

                             Level-1 Statistics
                             ------------------

Learnt routes information:
         Total IPv4 Learnt Routes in IPv4 Routing Table: 1
         Total IPv6 Learnt Routes in IPv6 Routing Table: 0

Imported routes information:
         IPv4 Imported Routes:
                        Static: 0       Direct: 0
                        ISIS:   0       BGP:    0
```

```
                        RIP:    0       OSPF:   0
        IPv6 Imported Routes:
                        Static: 0       Direct: 0
                        ISISv6: 0       BGP4+:  0
                        RIPng:  0       OSPFv3: 0

Lsp information:
                  LSP Source ID:          No. of used LSPs
                  0000.0000.0003                  002
```

Table 1-14 display isis statistics command output description

Field		Description
Statistics information for ISIS(*processid*)		Statistics for the IS-IS process
Level-1 Statistics		Level-1 Statistics
Level-2 Statistics		Level-2 Statistics
Learnt routes information		Number of learnt IPv4 routes Number of learnt IPv6 routes
Imported routes information	IPv4 Imported Routes	Redistributed IPv4 routes • Static • Direct • IS-IS • BGP • RIP • OSPF
	IPv6 Imported Routes	Redistributed IPv6 routes • Static • Direct • IS-ISv6 • BGP4+ • RIPng • OSPFv3
Lsp information		LSP information • LSP Source ID: ID of the source system • No. of used LSPs: number of used LSPs

domain-authentication-mode

Syntax

domain-authentication-mode { **simple** | **md5** } *password* [**ip** | **osi**]

undo domain-authentication-mode

View

IS-IS view

Default Level

2: System level

Parameters

simple: Specifies the simple authentication mode.

md5: Specifies the MD5 authentication mode.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plain text password can be a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **_(TT8F]Y\5SQ=^Q`MAF4<1!!**.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

Note

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description

Use the **domain-authentication-mode** command to specify the routing domain authentication mode and a password.

Use the **undo domain-authentication-mode** command to restore the default.

No routing domain authentication is configured by default

The configured password in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-2 packets.

Note that:

- All the backbone routers must have the same authentication mode and password.
- If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.

Related commands: **area-authentication-mode**, **isis authentication-mode**.

Examples

Specify the routing domain authentication mode as **simple** and password as **123456**.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] domain-authentication-mode simple 123456
```

filter-policy export (IS-IS view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View

IS-IS view

Default Level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter redistributed routes, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL commands* in the *Security Volume*.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter redistributed routes, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter redistributed routes, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

protocol: Filters routes redistributed from the routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

process-id: Process ID, in the range of 1 to 65535. It is optional only when the protocol is IS-IS, OSPF or RIP.

Description

Use the **filter-policy export** command to configure IS-IS to filter redistributed routes.

Use the **undo filter-policy export** command to disable IS-IS from filtering redistributed routes.

IS-IS does not filter redistributed routes by default.

Related commands: **filter-policy import**.

Examples

Reference ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 export
```

filter-policy import (IS-IS view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

View

IS-IS view

Default Level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter routes calculated from received LSPs, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL commands* in the *Security Volume*.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter routes calculated from received LSPs, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter routes calculated from received LSPs, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

Description

Use the **filter-policy import** command to configure IS-IS to filter routes calculated from received LSPs.

Use the **undo filter-policy import** command to disable IS-IS from filtering routes calculated from received LSPs.

IS-IS does not filter routes calculated from received LSPs by default.

Related commands: **filter-policy export**.

Examples

Reference ACL 2000 to filter routes calculated from received LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 import
```

flash-flood

Syntax

flash-flood [**flood-count** *flooding-count* | **max-timer-interval** *flooding-interval* | [**level-1** | **level-2**]] *

undo flash-flood [**level-1** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

flood-count *flooding-count*: Specifies the maximum number of LSPs to be flooded before the next SPF calculation, ranging from 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay (in milliseconds) of the flash flooding, ranging from 10 to 50000. The default is 10.

level-1: Enables flash flooding for **level-1**.

level-2: Enables fast-flooding for **level-2**.

Description

Use the **flash-flood** command to enable IS-IS LSP flash flooding.

Use the **undo flash-flood** command to disable IS-IS LSP flash flooding.

IS-IS LSP flash flooding is disabled by default.

If no level is specified, the command enables IS-IS LSP flash flooding for both Level-1 and Level-2.

Examples

Enable fast flooding and configure the maximum LSPs be sent as 10 and the delay time as 100 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

graceful-restart (IS-IS view)

Syntax

graceful-restart

undo graceful-restart

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **graceful-restart** command to enable IS-IS Graceful Restart capability.

Use the **undo graceful-restart** command to disable IS-IS Graceful Restart capability.

By default, IS-IS Graceful Restart capability is disabled.

Examples

Enable the Graceful Restart capability for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart
```

graceful-restart interval (IS-IS view)

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

View

IS-IS view

Default Level

2: System level

Parameters

interval-value: Graceful Restart interval, in the range 30 to 1800 seconds.

Description

Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 300 seconds.

Examples

Configure the Graceful Restart interval for IS-IS process 1 as 120 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart interval 120
```

graceful-restart suppress-sa

Syntax

graceful-restart suppress-sa

undo graceful-restart suppress-sa

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **graceful-restart suppress-sa** command to suppress the SA (Suppress-Advertisement) bit during restart.

Use the **undo graceful-restart suppress-sa** command to set the SA bit.

By default, the SA bit is set during restart.

Suppressing the SA bit is mainly for avoiding black hole route. If a router starts or reboots without keeping the local forwarding table, sending packets to the router may result in a severe packet loss. To avoid this, you can set the SA bit of the hello packet sent by the GR Restarter to 1. Upon receiving such hello packets, the GR Helpers will not advertise the GR Restarter through LSP.

Examples

Suppress the SA bit during Graceful Restart.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

import-route (IS-IS view)

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**cost** *cost* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route *protocol* [*process-id* | **all-processes**]

View

IS-IS view

Default Level

2: System level

Parameters

protocol: Redistributes routes from a routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

process-id: Process ID, in the range of 1 to 65535. It is available only when the protocol is IS-IS, OSPF or RIP.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows redistribution of IBGP routes. It is available when the protocol is BGP.

cost: Specifies a cost for redistributed routes.

The range of the cost depends on its style:

- For the styles of narrow, narrow-compatible and compatible, the cost ranges from 0 to 63.
- For the styles of wide, wide-compatible, the cost ranges from 0 to 16777215.

cost-type { **external** | **internal** }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route to be advertised is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow**, **narrow-compatible** or **compatible**.

level-1: Redistributes routes into the Level-1 routing table.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

route-policy *route-policy-name*: Redistributes only routes satisfying the matching conditions of a routing policy, the name of which is a string of 1 to 19 characters.

tag *tag*: Specifies a tag value for redistributed routes from 1 to 4294967295.

Description

Use the **import-route** command to redistribute routes from another routing protocol or another IS-IS process.

Use the **undo import-route** command to disable route redistribution from another routing protocol or another IS-IS process.

No route redistribution is configured by default.

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

Related commands: **import-route isis level-2 into level-1**.

Caution

- Using the **import-route bgp** command redistributes only EBGP routes. Using the **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes, but this may cause routing loops; be cautious with this command.
- Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.

Examples

Redistribute static routes and set the cost to 15.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route static cost 15
```

import-route isis level-2 into level-1

Syntax

import-route isis level-2 into level-1 [**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-2 into level-1

View

IS-IS view

Default Level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter routes from Level-2 to Level-1, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL commands* in the *Security Volume*.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter routes from Level-2 to Level-1, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter routes from Level-2 to Level-1, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy commands* in the *IP Routing Volume*.

tag *tag*: Specifies a tag value from 1 to 4294967295 for redistributed routes.

Description

Use the **import-route isis level-2 into level-1** command to enable route leaking from Level-2 to Level-1.

Use the **undo import-route isis level-2 into level-1** command to disable routing leaking.

No route leaking is configured by default.

Note that:

- You can specify a routing policy in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.
- If a filter policy is configured, only routes passing it can be advertised into the Level-1 area.

Related commands: **import-route**.

Examples

Enable route leaking from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route isis level-2 into level-1
```

import-route limit (IS-IS view)

Syntax

import-route limit *number*

undo import-route limit

View

IS-IS view

Default Level

2: System level

Parameters

number: Maximum number of redistributed Level 1/Level 2 IPv4 routes, in the range 1 to 128000.

Description

Use the **import-route limit** command to configure the maximum number of redistributed Level 1/Level 2 IPv4 routes.

Use the **undo import-route limit** command to restore the default.

By default, the maximum number of redistributed Level 1/Level 2 IPv4 routes is 128000.

Examples

Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv4 routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] import-route limit 1000
```

isis

Syntax

isis [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo isis [*process-id*]

View

System view

Default Level

2: System level

Parameters

process-id: Process ID, ranging from 1 to 65535. The default is 1.

vpn-instance-name: VPN instance name, a string of 1 to 31 characters.

Description

Use the **isis** command to enable an IS-IS process and specify an associated VPN instance and/or enter IS-IS view.

Use the **undo isis** command to disable an IS-IS process.

Related commands: **isis enable**, **network-entity**.

Examples

Enable IS-IS routing process 1, with the system ID being 0000.0000.0002, and area ID being 01.0001.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

isis authentication-mode

Syntax

isis authentication-mode { **simple** | **md5** } *password* [**level-1** | **level-2**] [**ip** | **osi**]

undo isis authentication-mode [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

simple: Specifies the simple authentication mode.

md5: Specifies the MD5 authentication mode.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plain text password can be a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **_(TT8F]Y\5SQ=^Q`MAF4<1!!**.

level-1: Sets the password for Level-1.

level-2: Sets the password for Level-2.

ip: Checks IP related fields in LSPs and SNPs.

osi: Checks OSI related fields in LSPs and SNPs.

Note

- This command is not available in loopback interface view.
- Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description

Use the **isis authentication-mode** command to set the IS-IS authentication mode and password for an interface.

Use the **undo isis authentication-mode** command to restore the default.

No neighbor relationship authentication is configured by default.

The password in the specified mode is inserted into all outgoing hello packets and is used for authenticating the incoming hello packets. Only the authentication succeeds can the neighbor relationship be formed.

Note that:

- For two routers to become neighbors, the same authentication mode and password must be specified at both ends.
- If you set a password without specifying a level, the password applies to both Level-1 and Level-2,
- If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.
- The **level-1** and **level-2** keywords are available only on the VLAN interfaces of switches after IS-IS is enabled on the interfaces with the **isis enable** command.

Related commands: **area-authentication-mode**, **domain authentication-mode.**

Examples

Set the plain text password **tangshi** for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple tangshi level-1
```

isis circuit-level

Syntax

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

View

Interface view

Default Level

2: System level

Parameters

level-1: Sets the circuit level to Level-1.

level-1-2: Sets the circuit level to Level-1-2.

level-2: Sets the circuit level to Level-2.

Description

Use the **isis circuit-level** command to set the circuit level for the interface.

Use the **undo isis circuit-level** command to restore the default.

An interface can establish either the Level-1 or Level-2 adjacency by default.

Note that:

For a Level-1 (Level-2) router, the circuit level can only be Level-1 (Level-2). For a Level-1-2 router, you need to specify a circuit level for a specific interface to form only the specified level neighbor relationship.

Related commands: **is-level**.

Examples

VLAN-interface 10 is connected to a non backbone router in the same area. Configure the circuit level of VLAN-interface 10 as Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-level level-1
```

isis circuit-type p2p

Syntax

isis circuit-type p2p

undo isis circuit-type

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **isis circuit-type p2p** command to configure the network type for an interface as P2P.

Use the **undo isis circuit-type** command to cancel the configuration.

By default, the network type of a switch's VLAN interface is broadcast.

Interfaces with different network types operate differently. For example, broadcast interfaces on a network need to elect a DIS and flood CSNP packets to synchronize the LSDBs, while P2P interfaces on a network need not elect a DIS and have a different LSDP synchronization mechanism.

If there are only two routers on a broadcast network, you can configure the network type of attached interfaces as P2P to avoid DIS election and CSNP flooding, saving network bandwidth and speeding up network convergence.

 **Note**

You can perform this configuration only for a broadcast network with only two attached routers.

Examples

Configure the network type of VLAN-interface 10 as P2P.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-type p2p
```

isis cost

Syntax

isis cost *value* [**level-1** | **level-2**]

undo isis cost [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

value: Specifies an IS-IS cost for the interface. The cost range differs with cost styles.

- For cost styles **narrow**, **narrow-compatible** and **compatible**, the cost ranges from 1 to 63.
- For cost styles **wide** and **wide-compatible**, the cost ranges from 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Description

Use the **isis cost** command to set the IS-IS cost of an interface.

Use the **undo isis cost** command to restore the default.

No cost is configured by default.

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

You are recommended to configure a proper IS-IS cost for each interface to guarantee correct route calculation.

Relate command: **circuit-cost**.

Examples

Configure the Level-2 IS-IS cost as 5 for VLAN-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis cost 5 level-2
```

isis dis-name

Syntax

isis dis-name *symbolic-name*

undo isis dis-name

View

Interface view

Default Level

2: System level

Parameters

symbolic-name: Specifies a DIS name, a string of 1 to 64 characters.

Description

Use the **isis dis-name** command to configure a name for a DIS to represent the pseudo node on a broadcast network.

Use the **undo isis dis-name** command to remove the configuration.

No name is configured for the DIS by default.

Note that this command takes effect only on a router that must have dynamic system ID to host name mapping enabled. This command is not supported on a Point-to-Point interface.

Note

This command is not available in loopback interface view.

Examples

Configure the DIS name as **LOCALAREA**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-name LOCALAREA
```

isis dis-priority

Syntax

isis dis-priority *value* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

value: Specifies a DIS priority for the interface, ranging from 0 to 127.

level-1: Applies the DIS priority to Level-1.

level-2: Applies the DIS priority to level-2.

Description

Use the **isis dis-priority** command to specify a DIS priority at a specified level for an interface.

Use the **undo isis dis-priority** command to restore the default priority of 64 for Level-1 and Level-2.

If neither level-1 nor level-2 is specified in this command, the DIS priority applies to both Level-1 and Level-2.

On an IS-IS broadcast network, a router should be elected as the DIS at each routing level. You can specify a DIS priority at a level for an interface. The greater the interface's priority is, the more likelihood it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest SNPA (Subnetwork Point of Attachment) address (SNPA addresses are MAC addresses on a broadcast network) becomes the DIS.

There is no backup DIS in IS-IS and the router with a priority of 0 can also participate in DIS election.

Note

This command is not available in loopback interface view.

Examples

Configure the level-2 DIS priority as 127 for VLAN-interface 10.

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

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Syntax

isis enable [*process-id*]

undo isis enable

View

Interface view

Default Level

2: System level

Parameters

process-id: Specifies a IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description

Use the **isis enable** command to enable an IS-IS process on the interface.

Use the **undo isis enable** command to disable IS-IS.

No IS-IS routing process is enabled on an interface by default.

Related commands: **isis**, **network-entity**.

Examples

Create IS-IS routing process 1, and enable the IS-IS routing process on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
```

isis mesh-group

Syntax

isis mesh-group { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

View

Interface view

Default Level

2: System level

Parameters

mesh-group-number: Mesh group number, ranging from 1 to 4294967295.

mesh-blocked: Blocks the interface, which sends LSPs only after receiving LSP requests.

Description

Use the **isis mesh-group** command to add the interface into a specified mesh group or block the interface.

Use the **undo isis mesh-group** command to restore the default.

By default, an interface does not belong to any mesh group.

For an interface not in a mesh group, it follows the normal process to flood the received LSPs to other interfaces. For the NBMA network with high connectivity and multiple point-to-point links, this will cause repeated LSP flooding and bandwidth waste.

After an interface is added to a mesh group, it will only flood a received LSP or a generated LSP to interfaces not belonging to the same mesh group.

If you block an interface, the interface can send LSPs only after receiving LSP requests.

Note

- The mesh-group feature is only available for a point-to-point link interface.
- This command is not available in loopback interface view.

Examples

Add IS-IS enabled VLAN-interface 10 to the mesh-group 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis mesh-group 3
```

isis silent

Syntax

isis silent

undo isis silent

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **isis silent** command to disable the interface from sending and receiving IS-IS packets.

Use the **undo isis silent** command to restore the default.

By default, an interface is not disabled from sending and receiving IS-IS packets.

 **Note**

The feature is not supported on the loopback interface.

Examples

Disable VLAN-interface 10 from sending and receiving IS-IS packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis silent
```

isis small-hello

Syntax

isis small-hello

undo isis small-hello

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **isis small-hello** command to configure the interface to send small hello packets without CLVs.

Use the **undo isis small-hello** command to restore the default.

An interface sends standard hello packets by default.

 **Note**

This command is not available in loopback interface view.

Examples

Configure VLAN-interface 10 to send small Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis small-hello
```

isis timer csnp

Syntax

isis timer csnp *seconds* [**level-1** | **level-2**]

undo isis timer csnp [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

seconds: Specifies on the DIS of a broadcast network the interval in seconds for sending CSNP packets, ranging from 1 to 600.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Description

Use the **isis timer csnp** command to specify on the DIS of a broadcast network the interval for sending CSNP packets.

Use the **undo isis timer csnp** command to restore the default.

The default CSNP interval is 10 seconds.

Note

- If no level is specified, the CSNP interval applies to both Level-1 and Level-2.
- This command only applies to the DIS of a broadcast network, which sends CSNP packets periodically for LSDB synchronization.

Examples

Configure Level-2 CSNP packets to be sent every 15 seconds over VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer csnp 15 level-2
```

isis timer hello

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

seconds: Specifies the interval in seconds for sending hello packets, ranging from 3 to 255.

level-1: Specifies the interval for sending Level-1 hello packets.

level-2: Specifies the interval for sending Level-2 hello packets.

Description

Use the **isis timer hello** command to specify the interval for sending hello packets.

Use the **undo isis timer hello** command to restore the default.

The default hello interval is 10 seconds.

Note

- Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify an interval for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify an interval for two levels respectively.
- As the shorter the interval is, the more system resources will be occupied, you should configure a proper interval as needed.
- If no level is specified, the hello interval applies to both Level-1 and Level-2.

Related commands: **isis timer holding-multiplier**.

Examples

Configure Level-2 Hello packets to be sent every 20 seconds over VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer hello 20 level-2
```

isis timer holding-multiplier

Syntax

isis timer holding-multiplier *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [**level-1** | **level-2**]

View

Interface view

Default Level

2: System level

Parameters

value: Number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.

Note

This command is not available in loopback interface view.

Description

Use the **isis timer holding-multiplier** command to specify the IS-IS hello multiplier.

Use the **undo isis timer holding-multiplier** command to restore the default.

The default IS-IS hello multiplier is 3.

If no level is specified, the hello multiplier applies to the current level.

With the IS-IS hello multiplier configured, a router can uses hello packets to notify its neighbor router of the adjacency hold time (hello multiplier times hello interval). If the neighbor router receives no hello packets from this router within the hold time, it declares the adjacency down. You can adjust the adjacency hold time by changing the hello multiplier or the hello interval on an interface.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify a hello multiplier for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify Level-1 or Level-2.

Related commands: **isis timer hello**.

Examples

Configure the number of Level-2 Hello intervals as 6 for interface VLAN-interface, that is, if no Hello packet is received from the interface within 6 hello intervals, the IS-IS neighbor is considered dead.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer holding-multiplier 6
```

isis timer lsp

Syntax

isis timer lsp *time* [**count** *count*]

undo isis timer lsp

View

Interface view

Default Level

2: System level

Parameters

time: Specifies the minimum interval in milliseconds for sending link-state packets, ranging from 1 to 1000.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000. The default is 5.

Description

Use the **isis timer lsp** command to configure the minimum interval for sending LSPs on the interface and specify the maximum LSPs that can be sent per time.

Use the **undo isis timer lsp** command to restore the default of 33ms.

Related commands: **isis timer retransmit**.

Note

This command is not available in loopback interface view.

Examples

Configure the interval as 500 milliseconds for sending LSPs on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer lsp 500
```

isis timer retransmit

Syntax

isis timer retransmit *seconds*

undo isis timer retransmit

View

Interface view

Default Level

2: System level

Parameters

seconds: Specifies the interval in seconds for retransmitting LSP packets, ranging from 1 to 300.

Description

Use the **isis timer retransmit** command to configure the interval for retransmitting LSP packets over a point-to-point link.

Use the **undo isis timer retransmit** command to restore the default.

By default, the retransmission interval is 5 seconds.

A P2P link requires a response to a sent LSP. If no response is received within the retransmission interval, the LSP is retransmitted.

You need not use this command over a broadcast link where CNSPs are broadcast periodically.

Related commands: **isis timer lsp**.

 **Note**

- This command is not available in loopback interface view.
- Configure a proper retransmission interval to avoid unnecessary retransmissions.

Examples

Configure the LSP retransmission interval as 10 seconds for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer retransmit 10
```

is-level

Syntax

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

View

IS-IS view

Default Level

2: System level

Parameters

level-1: Configures the router to work on Level-1, which means it only calculates routes within the area, and maintains the L1 LSDB.

level-1-2: Configures the router to work on Level-1-2, which means it calculates routes and maintains the LSDBs for both L1 and L2.

level-2: Configures the router to work on Level-2, which means it calculates routes and maintains the LSDB for L2 only.

Description

Use the **is-level** command to specify the IS level.

Use the **undo is-level** command to restore the default.

The default IS level is **level-1-2**.

You can configure all the routers as either Level-1 or Level-2 if there is only one area, because there is no need for all routers to maintain two identical databases at the same time. If the only area is an IP network, you are recommended to configure all the routers as Level-2 for scalability.

Related commands: **isis circuit-level**.

Examples

Configure the router to work in Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-level level-1
```

is-name

Syntax

is-name *sys-name*

undo is-name

View

IS-IS view

Default Level

2: System level

Parameters

symbolic-name: Specifies a host name for the local IS, a string of 1 to 64 characters.

Description

Use the **is-name** command to specify a host name for the IS to enable dynamic system ID to hostname mapping.

Use the **undo is-name** command to disable dynamic system ID to hostname mapping.

Dynamic system ID to hostname mapping is not enabled by default.

Examples

Configure a host name for the local IS.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

is-name map

Syntax

is-name map *sys-id map-sys-name*

undo is-name map *sys-id*

View

IS-IS view

Default Level

2: System level

Parameters

sys-id: System ID or pseudonode ID of a remote IS.

map-sys-name: Specifies a host name for the remote IS, a string of 1 to 64 characters.

Description

Use the **is-name map** command to configure a system ID to host name mapping for a remote IS.

Use the **undo is-name map** command to remove the mapping.

Each remote IS system ID corresponds to only one name.

Examples

Map the host name RUTB to the system ID 0000.0000.0041 of the remote IS.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

is-snmp-traps enable

Syntax

is-snmp-traps enable

undo is-snmp-traps

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **is-snmp-traps enable** command to enable the SNMP Trap function of IS-IS.

Use the **undo is-snmp-traps** command to disable this function.

SNMP Trap is enabled by default.

Examples

Enable SNMP Trap.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-snmp-traps enable
```

log-peer-change (IS-IS view)

Syntax

log-peer-change

undo log-peer-change

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **log-peer-change** command to enable the logging of IS-IS neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

After the logging is enabled, information about IS-IS adjacency state changes is sent to the configuration terminal.

Examples

Enable logging on the IS-IS adjacency state changes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] log-peer-change
```

lsp-fragments-extend

Syntax

lsp-fragments-extend [[**level-1** | **level-2** | **level-1-2**] | [**mode-1** | **mode-2**]] *

undo lsp-fragments-extend

View

IS-IS view

Default Level

2: System level

Parameters

mode-1: Fragment extension mode 1, used on a network where some routers do not support LSP fragment extension.

mode-2: Fragment extension mode 2, used on a network where all routers support LSP fragment extension.

level-1: Applies the fragment extension mode to Level-1 LSPs.

level-2: Applies the fragment extension mode to Level-2 LSPs.

level-1-2: Applies the fragment extension mode to both Level-1 and Level-2 LSPs.

Description

Use the **lsp-fragments–extend** command to enable an LSP fragment extension mode for a level.

Use the **undo lsp-fragments–extend** command to disable LSP fragment extension for a level.

LSP fragment extension is disabled by default.

Note that:

- If no mode is specified, LSP fragment extension mode 1 is enabled.
- If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.

Examples

Enable LSP fragment extension mode 1 for Level-2.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-fragments-extend mode-1 level-2
```

lsp-length originate

Syntax

lsp-length originate *size* [**level-1** | **level-2**]

undo lsp-length originate [**level-1** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

size: Specifies the maximum size in bytes of LSP packets, ranging from 512 to 16384.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.

Description

Use the **lsp-length originate** command to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use the **undo lsp-length originate** command to restore the default.

By default, the maximum size of generated Level-1 and Level-2 LSPs is 1497 bytes.

 **Note**

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Examples

Configure the maximum size of the generated Level-2 LSPs as 1024 bytes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length originate 1024 level-2
```

lsp-length receive

Syntax

lsp-length receive *size*

undo lsp-length receive

View

IS-IS view

Default Level

2: System level

Parameters

size: Maximum size of received LSPs, in the range of 512 to 16384 bytes.

Description

Use the **lsp-length receive** command to configure the maximum size of received LSPs.

Use the **undo lsp-length receive** command to restore the default.

By default, the maximum size of received LSPs is 1497 bytes.

Examples

Configure the maximum size of received LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing (IS-IS view)

Syntax

maximum load-balancing *number*

undo maximum load-balancing

View

IS-IS view

Default Level

2: System level

Parameters

number: Maximum number of equal-cost routes for load balancing, in the range 1 to 4..

Description

Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost load balanced routes is 4.

Examples

Configure the maximum number of equal-cost load-balanced routes as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-isis-100] undo maximum load-balancing
```

network-entity

Syntax

network-entity *net*

undo network-entity *net*

View

IS-IS view

Default Level

2: System level

Parameters

net: Network Entity Title (NET) in the format of X…X.XXXX....XXXX.00, with the first part X…X being the area address, the middle part XXXX....XXXX (a total of 12 “X”) being the router’s system ID and the last part 00 being SEL.

Description

Use the **network-entity** command to configure the Network Entity Title for an IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

No NET is configured by default.

Related commands: **isis**, **isis enable**.

Examples

Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

preference (IS-IS view)

Syntax

preference { **route-policy** *route-policy-name* | *preference* } *

undo preference

View

IS-IS view

Default Level

2: System level

Parameters

preference: Specifies the preference for IS-IS protocol, ranging from 1 to 255.

route-policy *route-policy-name*: Routing policy name, a string of 1 to 19 characters. The preference applies to routes passing the routing policy.

Description

Use the **preference** command to configure the preference for IS-IS.

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

By default, IS-IS preference is 15.

If a routing policy is specified in this command, the preference (if any) set by the routing policy applies to those matched routes. Other routes use the preference set by the **preference** command.

When a router runs multiple routing protocols at the same time, the system will configure a preference to each routing protocol. If several protocols find routes to the same destination, the route of the routing protocol with the highest preference is selected.

Examples

Configure the preference of IS-IS protocol as 25.

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1] preference 25
```

reset isis all

Syntax

reset isis all [*process-id* | **vpn-instance** *vpn-instance-name*]

View

User view

Default Level

3: Manage level

Parameters

process-id: Clears the data structure information of an IS-IS process numbered from 1 to 65535.

vpn-instance-name: Clears the data structure information of a VPN instance named with a string of 1 to 31 characters.

Description

Use the **reset isis all** command to clear all IS-IS data structure information.

No data structure information is cleared by default.

This command is used when the LSP needs to be updated immediately. For example, after performing the **area-authentication-mode** and **domain-authentication-mode** commands, you can use this command to clear old LSPs.

Related commands: **area-authentication-mode**, **domain authentication-mode.**

Examples

Clear all IS-IS data structure information.

```
<Sysname> reset isis all
```

reset isis peer

Syntax

reset isis peer *system-id* [*process-id* | **vpn-instance** *vpn-instance-name*]

View

User view

Default Level

3: Manage level

Parameters

system-id: Specifies the system ID of an IS-IS neighbor.

process-id: Clears the data structure information of an IS-IS process with an ID from 1 to 65535.

vpn-instance-name: Clears the data structure information of a VPN instance named with a string of 1 to 31 characters.

Description

Use the **reset isis peer** command to clear the data structure information of a specified IS-IS neighbor.

This command is used when you need to re-establish an IS-IS neighbor relationship.

Examples

Clear the data structure information of the neighbor with the system ID 0000.0c11.1111.

```
<Sysname> reset isis peer 0000.0c11.1111
```

set-overload

Syntax

set-overload [**on-startup** [[**start-from-nbr** *system-id* [*timeout1* [*nbr-timeout*]]] | *timeout2*] [**allow** { **interlevel** | **external** } *]

undo set-overload

View

IS-IS view

Default Level

2: System level

Parameters

on-startup: Sets the overload bit upon system startup.

start-from-nbr *system-id*: Starts the *nbr-timeout* timer when the router begins to establish the neighbor relationship with the neighbor. If the neighbor relationship is formed within the *nbr-timeout* interval, IS-IS keeps the overload bit set; if not, the bit is cleared. *system-id* specifies the neighbor.

timeout1: IS-IS keeps the overload bit set within the *timeout1* interval after the neighbor relationship is formed within the *nbr-timeout* interval. The *timeout1* interval is in the range 5 to 86400 seconds and defaults to 600 seconds.

nbr-timeout: The timer is started when the router begins to establish the neighbor relationship with the neighbor after system startup. The timer has an interval from 5 to 86400 seconds. The default is 1200 seconds.

timeout2: Sets the overload bit within the *timeout2* interval after system startup. The interval is in the range 5 to 86400 seconds and defaults to 600 seconds.

allow: Allows advertising address prefixes. By default, no address prefixes are allowed to be advertised when the overload bit is set.

interlevel: Allows advertising IP address prefixes learnt from different IS-IS levels with the **allow** keyword specified.

external: Allows advertising IP address prefixes redistributed from other routing protocols with the **allow** keyword specified.

Description

Use the **set-overload** command to set the overload bit.

Use the **undo set-overload** command to clear the overload bit.

The overload bit is not set by default.

Note that:

- If the **on-startup** keyword is not specified, the command sets the overload bit immediately until the **undo set-overload** command is executed.
- If the **on-startup** keyword is specified, IS-IS sets the overload bit upon system startup and keeps it set within the *timeout2* interval.
- If both **on-startup** and **start-from-nbr** *system-id* are specified, IS-IS sets the overload bit from system startup to when the neighbor relationship with the specified neighbor is formed within the *nbr-timeout* interval, and from then on, IS-IS keeps the overload bit set within the *timeout1* interval. If the neighbor relationship with the specified neighbor is not formed within the *nbr-timeout* interval, the overload bit is cleared.

Examples

Set overload flag on the current router.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] set-overload
```

summary (IS-IS view)

Syntax

summary *ip-address* { *mask* | *mask-length* } [**avoid-feedback** | **generate_null0_route** | [**level-1** | **level-1-2** | **level-2**] | **tag** *tag*] *

undo summary *ip-address* { *mask* | *mask-length* } [**level-1** | **level-1-2** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

ip-address: Destination IP address of the summary route.

mask: Mask of the destination IP address, in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32.

avoid-feedback: Avoids learning summary routes by route calculation.

generate_null0_route: Generate the Null 0 route to avoid routing loops.

level-1: Summarize only the routes redistributed to Level-1.

level-1-2: Summarizes the routes redistributed to both Level-1 and Level-2.

level-2: Summarizes only the routes redistributed to Level-2.

tag *tag*: Specifies a management tag, in the range of 1 to 4294967295.

Description

Use the **summary** command to configure a summary route.

Use the **undo summary** command to remove a summary route.

No summarization is configured by default.

If no level is specified, only the **level-2** routes will be summarized by default.

You can summarize multiple contiguous networks into a single network to reduce the size of the routing table, as well as that of LSP and LSDB generated by the router. It is allowed to summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of those summarized routes.

Note that the router summarizes only routes in local LSPs.

Examples

Configure a summary route of 202.0.0.0/8.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] summary 202.0.0.0 255.0.0.0
```

timer lsp-generation

Syntax

timer lsp-generation *maximum-interval* [*initial-interval* [*second-wait-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [**level-1** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

maximum-interval: Maximum wait interval in seconds for generating IS-IS LSPs, in the range 1 to 120.

initial-interval: Initial wait interval in milliseconds before generating the first IS-IS LSP, in the range 10 to 60000. The default is 0.

second-wait-interval: Wait interval in milliseconds before generating the second LSP, in the range 10 to 60000. The default is 0.

level-1: Applies the intervals to Level-1.

level-2: Applies the intervals to Level-2 .If no level is specified, the specified intervals apply to both Level-1 and Level-2.

Description

Use the **timer lsp-generation** command to specify the wait interval before generating IS-IS LSPs.

Use the **undo timer lsp-generation** command to restore the default.

By default, the wait interval before LSP generation is 2 seconds.

Note that:

1) If only the maximum interval is specified, IS-IS waits the maximum interval before generating an LSP.

2) If both the maximum and initial intervals are specified:

- IS-IS waits the initial interval before generating the first LSP.
- If the network topology is unstable, that is, triggers occur at intervals shorter than the maximum interval, IS-IS waits the maximum interval before generating the first LSP until the network topology is stable.

3) If the maximum, initial, and second wait intervals are specified:

- IS-IS waits the initial interval before generating the first LSP.
- If the network topology is unstable, that is, triggers occur at intervals shorter than the maximum interval,, IS-IS waits the *second-wait-interval* before generating the second LSP and penalty is applied on the wait interval before generating the next LSP. That is, for each subsequent trigger, the wait interval before generating the LSP will be two times the previous wait interval until the maximum interval is reached.
- After the network topology is stable; that is, triggers occur at intervals greater than the maximum interval, the wait interval before generating LSPs is restored to the initial interval.

Examples

Set the maximum, initial, and second wait intervals to 10 seconds, 100 milliseconds and 200 milliseconds respectively.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 10 100 200
```

Set the LSP generation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 15
```

timer lsp-max-age

Syntax

timer lsp-max-age *second*s

undo timer lsp-max-age

View

IS-IS view

Default Level

2: System level

Parameters

seconds: Specifies the LSP maximum aging time in seconds, ranging from 1 to 65535.

Description

Use the **timer lsp-max-age** command to set the LSP maximum age in the LSDB.

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

The default LSP maximum age is 1200 seconds.

Related commands: **timer lsp-refresh**.

Examples

Set the maximum LSP age to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax

timer lsp-refresh *seconds*

undo timer lsp-refresh

View

IS-IS view

Default Level

2: System level

Parameters

seconds: LSP refresh interval in seconds, ranging from 1 to 65534.

Description

Use the **timer lsp-refresh** command to configure the LSP refresh interval.

Use the **undo timer lsp-refresh** to restore the default.

The default LSP refresh interval is 900 seconds.

Related commands: **timer lsp-max-age**.

Note

To refresh LSPs before they are aged out, the interval configured by the **timer lsp-refresh** command must be smaller than that configured by the **timer lsp-max-age** command.

Examples

Configure the LSP refresh interval as 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-refresh 1500
```

timer spf

Syntax

timer spf *maximum-interval* [*initial-interval* [*second-interval*]]

undo timer spf

View

IS-IS view

Default Level

2: System level

Parameters

maximum-interval: Maximum SPF calculation interval in seconds, ranging from 1 to 120.

initial-interval: Wait interval before the first SPF calculation, in milliseconds, ranging from 10 to 60000.

second-interval: Wait interval before the second SPF calculation, in milliseconds, ranging from 10 to 60000.

Description

Use the **timer spf** command to set the SPF calculation interval.

Use the **undo timer spf** command to restore the default.

The default IS-IS SPF calculation interval is 10 seconds.

Note that:

1) If only the maximum interval is specified, IS-IS waits the maximum interval before performing the SPF calculation.
2) If both the maximum and initial intervals are specified:

- IS-IS waits the initial interval before performing the first SPF calculation.
- When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable and IS-IS waits the maximum interval before performing the SPF calculation unitl the topology is stable.

3) If maximum-interval, initial-interval, and second-interval are specified:

- IS-IS waits the initial interval before performing the first SPF calculation.
- When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable, IS-IS will wait the *second-interval* before performing the second SPF calculation and penalty is applied on the wait interval for the next SPF calculation. That is, for each subsequent trigger, the wait interval before SPF calculation will be two times the previous wait interval until the maximum interval is reached.
- After the network topology becomes stable; that is, triggers occur at intervals greater than the maximum interval, the wait interval before SPF calculation is restored to the initial interval.

Examples

Configure the maximum SPF calculation interval as 10 seconds, the wait interval before the first SPF calculation as 100 milliseconds, and the wait interval before the second SPF calculation as 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 10 100 200
```

Configure the maximum SPF calculation interval as 15 seconds.

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1]timer spf 15
```

virtual-system

Syntax

virtual-system *virtual-system-id*

undo virtual-system *virtual-system-id*

View

IS-IS view

Default Level

2: System level

Parameters

virtual-system-id: Virtual system ID of the IS-IS process.

Description

Use the **virtual-system** command to configure a virtual system ID for the IS-IS process. Use the **undo virtual-system** command to remove a virtual system ID.

Up to 50 virtual system IDs can be configured for the IS-IS process.

Examples

Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] virtual-system 2222.2222.2222
```

Table of Contents

1 BGP Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

BGP Configuration Commands

Note

For more information about routing policy configuration commands in this document, refer to *Routing Policy Commands* in the *IP Routing Volume*.

aggregate

Syntax

aggregate *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* | *mask-length* }

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

ip-address: Summary address.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range 0 to 32.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name:* Sets the attributes of the summary route according to the routing policy The routing policy name is a string of 1 to 19 characters.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a string of 1 to 19 characters.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

Table 1-1 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the **peer filter-policy** command.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the **if-match** clause of the **route-policy** command.
origin-policy	Selects only routes satisfying the routing policy for route summarization.
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the **peer route-policy** command.

Description

Use the **aggregate** command to create a summary route in the BGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

Examples

In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

In BGP-VPN instance view, create a summary of 192.213.0.0/16 in BGP routing table (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] aggregate 192.213.0.0 255.255.0.0
```

balance (BGP/BGP-VPN instance view)

Syntax

balance *number*

undo balance

View

BGP view/VPN instance view

Default Level

2: System level

Parameters

number: Number of BGP routes for load balancing, in the range 1 to 4. When it is set to 1, load balancing is disabled.

Description

Use the **balance** command to configure the number of BGP routes for load balancing.

Use the **undo balance** command to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display bgp routing-table**.

Examples

In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

In BGP-VPN instance view, set the number of routes participating in BGP load balancing to 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] balance 2
```

bestroute as-path-neglect (BGP/BGP-VPN instance view)

Syntax

bestroute as-path-neglect

undo bestroute as-path-neglect

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute as-path-neglect** command to configure BGP not to consider the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure BGP to consider the AS_PATH during best route selection.

By default, BGP considers the AS_PATH during best route selection.

Examples

In BGP view, ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

In BGP-VPN instance view, ignore AS_PATH in route selection (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute as-path-neglect
```

bestroute compare-med (BGP/BGP-VPN instance view)

Syntax

bestroute compare-med

undo bestroute compare-med

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

Examples

In BGP view, enable the comparison of MEDs for paths from each AS when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

In BGP-VPN instance view, enable the comparison of MED for paths from each AS when selecting the best route. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute compare-med
```

bestroute med-confederation (BGP/BGP-VPN instance view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers within the confederation. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute med-confederation
```

bgp

Syntax

bgp *as-number*

undo bgp [*as-number*]

View

System view

Default Level

2: System level

Parameters

as-number: Specifies the local AS number from 1 to 65535.

Description

Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, BGP is not enabled.

Examples

Enable BGP and set local AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]
```

compare-different-as-med (BGP/BGP-VPN instance view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If several paths to one destination are available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples

In BGP view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] compare-different-as-med
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers in different ASs (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] compare-different-as-med
```

confederation id

Syntax

confederation id *as-number*

undo confederation id

View

BGP view

Default Level

2: System level

Parameters

as-number: Number of the AS that contains multiple sub-ASs, in the range 1 to 65535.

Description

Use the **confederation id** command to configure a confederation ID.

Use the **undo confederation id** command to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

Examples

Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation while the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
```

```
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax

confederation nonstandard

undo confederation nonstandard

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **confederation nonstandard** command to make the router compatible with routers not compliant with RFC3065 in the confederation.

Use the **undo confederation nonstandard** command to restore the default.

By default, all routers in the confederation comply with RFC3065.

All devices should be configured with this command to interact with those nonstandard devices in the confederation.

Related commands: **confederation id** and **confederation peer-as**.

Examples

AS100 contains routers not compliant with RFC3065 and comprises two sub-ASs, 64000 and 65000.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

confederation peer-as

Syntax

confederation peer-as *as-number-list*

undo confederation peer-as [*as-number-list*]

View

BGP view

Default Level

2: System level

Parameters

as-number-list: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = a*s-number* &<1-32>, in which a*s-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

Description

Use the **confederation peer-as** command to specify confederation peer sub-ASs.

Use the **undo confederation peer-as** command to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, the **confederation id** command must be used to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

Examples

Specify confederation peer sub ASs 2000 and 2001.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] confederation id 10
[Sysname-bgp] confederation peer-as 2000 2001
```

dampening (BGP/BGP-VPN instance view)

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

half-life-reachable: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

half-life-reachable, half-life-unreachable, reuse, suppress and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description

Use the **dampening** command to enable BGP route dampening and/or configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter** and **display bgp routing-table flap-info**.

Examples

In BGP view, configure BGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

In BGP-VPN instance view, configure BGP route dampening (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] dampening 15 15 1000 2000 10000
```

default ipv4-unicast

Syntax

default ipv4-unicast

undo default ipv4-unicast

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **default ipv4-unicast** command to enable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

Use the **undo default ipv4-unicast** command to disable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

The use of IPv4 unicast address family is enabled by default.

Note that:

- The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established after it is executed.
- The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established using the **peer as-number** command.
- After executing the **undo default ipv4-unicast** command, you can use the **peer enable** command to enable the use of IPv4 address family for a peer.

Examples

Enable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default ipv4-unicast
```

default local-preference (BGP/BGP-VPN instance view)

Syntax

default local-preference *value*

undo default local-preference

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

value: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Using this command can affect BGP route selection.

Examples

In BGP view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default local-preference 180
```

In BGP-VPN instance view, set the default local preference to 180 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default local-preference 180
```

default med (BGP/BGP-VPN instance view)

Syntax

default med *med-value*

undo default med

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

med-value: Default MED value, in the range 0 to 4294967295.

Description

Use the **default med** command to specify a default MED value.

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

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

Examples

In BGP view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25
```

In BGP-VPN instance view, configure the default MED as 25 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default med 25
```

default-route imported (BGP/BGP-VPN instance view)

Syntax

default-route imported

undo default-route imported

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **default-route imported** command to allow default route redistribution into the BGP routing table.

Use the **undo default-route imported** command to disallow the redistribution.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route.**

Examples

In BGP view, allow default route redistribution from OSPF into BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1
```

In BGP-VPN instance view, enable redistributing default route from OSPF into BGP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default-route imported
[Sysname-bgp-vpn1] import-route ospf 1
```

display bgp group

Syntax

display bgp group [*group-name*]

View

Any view

Default Level

1: Monitor level

Parameters

group-name: Peer group name, a string of 1 to 47 characters.

Description

Use the **display bgp group** command to display peer group information.

Examples

Display the information of the peer group **aaa**.

```
<Sysname> display bgp group aaa
 BGP peer-group is aaa
 Remote AS 200
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  2.2.2.1         4   200        0        0     0       0 00:00:35 Active
```

Table 1-2 display bgp group command output description

Field	Description
BGP peer-group	Name of the BGP peer group
Remote AS	AS number of peer group
type	Type of the BGP peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum prefixes allowed to receive from the peer group
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisements
Peer Preferred Value	Preferred value specified for the routes from the peer

Field	Description
No routing policy is configured	No routing policy is configured.
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on the peer
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of the session/the lasting time of the current state (when no session is established)
State	State machine state of the peer

display bgp network

Syntax

display bgp network

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp network** command to display routing information advertised with the **network** command.

Examples

Display routing information advertised with the **network** command.

```
<Sysname> display bgp network

  BGP Local Router ID is 10.1.4.2.
  Local AS Number is 400.
  Network          Mask            Route-policy        Short-cut

  100.1.2.0        255.255.255.0
  100.1.1.0        255.255.255.0                       Short-cut
```

Table 1-3 display bgp network command output description

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Mask	Mask
Route-policy	Routing policy
Short-cut	Short-cut route

display bgp paths

Syntax

display bgp paths [*as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

Description

Use the **display bgp paths** command to display information about BGP AS paths.

Examples

Display information about BGP paths matching the AS path regular expression.

```
<Sysname> display bgp paths ^200

    Address       Hash    Refcount  MED         Path/Origin
    0x5917100     11      1          0          200 300i
```

Table 1-4 display bgp paths command output description

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that reference the path
MED	MED of the path
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops

Field	Description	
Origin	Origin attribute of the path:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means.

display bgp peer

Syntax

display bgp peer [*ip-address* { **log-info** | **verbose** } | *group-name* **log-info** | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: IP address of an peer to be displayed, in dotted decimal notation.

group-name: Name of a peer group to be displayed, a string of 1 to 47 characters.

log-info: Displays the log information of the specified peer.

verbose: Displays the detailed information of the peer/peer group.

Description

Use the **display bgp peer** command to display peer/peer group information.

Examples

Display the detailed information of the peer 10.110.25.20.

```
<Sysname> display bgp peer 10.110.25.20 verbose

          Peer: 10.110.25.20 Local: 2.2.2.2
          Type: EBGP link
          BGP version 4, remote router ID 1.1.1.1
          BGP current state: Established, Up for 00h01m51s
          BGP current event: RecvKeepalive
          BGP last state: OpenConfirm
          Port:  Local - 1029     Remote - 179
          Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
          Received  : Active Hold Time: 180 sec
          Negotiated: Active Hold Time: 180 sec
          Peer optional capabilities:
          Peer support bgp multi-protocol extended
```

```
        Peer support bgp route refresh capability
        Address family IPv4 Unicast: advertised and received

Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0
BFD: Enabled

Routing policy configured:
No routing policy is configured
```

Table 1-5 display bgp peer command output description

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type
BGP version	BGP version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Previous state of the peer
Port	TCP port numbers of the local router and its peer
Configured: Active Hold Time	Local holdtime interval
Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval
Peer optional capabilities	Optional capabilities supported by the peer, including BGP multiprotocol extensions and route refresh
Address family IPv4 Unicast	Routes are advertised and received in IPv4 unicasts.
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Minimum time between advertisement runs	Minimum route advertisement interval

Field	Description
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer
BFD	BFD is enabled or disabled.
Routing policy configured	Local routing policy

display bgp routing-table

Syntax

display bgp routing-table [*ip-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-prefixes: Matches the longest prefix.

Description

Use the **display bgp routing-table** command to display specified BGP routing information in the BGP routing table.

Examples

Display BGP routing table information.

```
<Sysname> display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  40.40.40.0/24     20.20.20.1                              0       200 300i
```

Table 1-6 display bgp routing command output description

Field	Description	
Total Number of Routes	Total Number of Routes	
BGP Local router ID	BGP local router ID	
Status codes	Status codes: * – valid > – best d – damped h – history i – internal (IGP) s – summary suppressed (suppressed) S – Stale	
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by some other means)	
Network	Destination network address	
Next Hop	Next hop IP address	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
PrefVal	Preferred value of the route	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
PrefVal	Preferred value	
Ogn	Origin attribute of the route, which can be one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes injected with the **network** command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means.

display bgp routing-table as-path-acl

Syntax

display bgp routing-table as-path-acl *as-path-acl-number*

View

Any view

Default Level

1: Monitor level

Parameters

as-path-acl-number: Displays routing information permitted by the AS path ACL, which is specifies with a number from 1 to 256.

Description

Use the **display bgp routing as-path-acl** command to display BGP routes permitted by an as-path ACL.

Examples

Display BGP routes permitted by AS path ACL 1.

```
<Sysname> display bgp routing-table as-path-acl 1

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf      PrefVal Path/Ogn

*>  40.40.40.0/24     30.30.30.1     0                    0      300i
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table cidr

Syntax

display bgp routing-table cidr

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table cidr** command to display BGP CIDR (Classless Inter-Domain Routing) routing information.

Examples

Display BGP CIDR routing information.

```
<Sysname> display bgp routing-table cidr
```

```
 Total Number of Routes: 1

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop         MED        LocPrf     PrefVal Path/Ogn

*>  40.40.40.0/24    30.30.30.1      0                     0       300i
```

Refer to Table 1-6 for description on the above fields.

display bgp routing-table community

Syntax

display bgp routing-table community [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View

Any view

Default Level

1: Monitor level

Parameters

aa:nn: Community number. Both aa and nn are in the range 0 to 65535.

&<1-13>: Argument before it can be entered up to 13 times.

no-advertise: Displays BGP routes that cannot be advertised to any peer.

no-export: Displays BGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays BGP routes that cannot be advertised out the AS or to other sub ASs in the configured confederation.

whole-match: Displays the BGP routes exactly matching the specified community attribute.

Description

Use the **display bgp routing community** command to display BGP routing information with the specified BGP community attribute.

Examples

Display BGP routing information with the specified BGP community.

```
<Sysname> display bgp routing-table community 11:22

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  10.10.10.0/24     0.0.0.0         0                  0      i
 *>  40.40.40.0/24      20.20.20.1                            0       200 300i
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table community-list

Syntax

display bgp routing-table community-list { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View

Any view

Default Level

1: Monitor level

Parameters

basic-community-list-number: Specifies a basic community-list number from 1 to 99.

adv-community-list-number: Specifies an advanced community-list number from 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

Description

Use the **display bgp routing-table community-list** command to display BGP routing information matching the specified BGP community list.

Examples

Display BGP routing information matching BGP community list 100.

```
<Sysname> display bgp routing-table community-list 100
 BGP Local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
      Network            NextHop        Metric     LocPrf    PrefVal Path

 *>   3.3.3.0/30         1.2.3.4                             0       ?
 *>   4.4.0.0/20         1.2.3.4                             0       ?
 *>   4.5.6.0/26         1.2.3.4                             0       ?



 BGP Local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn
 *>   3.3.3.0/30         1.2.3.4                              0       ?
 *>   4.4.0.0/20         1.2.3.4                              0       ?
 *>   4.5.6.0/26         1.2.3.4                              0       ?
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table dampened

Syntax

display bgp routing-table dampened

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table dampened** command to display dampened BGP routes.

Examples

Display dampened BGP routes.

```
<Sysname> display bgp routing-table dampened
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            From              Reuse     Path/Origin
 *d  77.0.0.0           12.1.1.1          00:29:20  100?
```

Table 1-7 display bgp routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to Table 1-6 for description on the other fields above.

display bgp routing-table dampening parameter

Syntax

display bgp routing-table dampening parameter

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table dampening parameter** command to display BGP route dampening parameters.

Related commands: **dampening**.

Examples

Display BGP route dampening parameters.

```
<Sysname> display bgp routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 Reach HalfLife Time(in  second)  : 900
 Unreach HalfLife Time(in  second): 900
 Suppress-Limit                   : 2000
```

Table 1-8 display bgp routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Limit for a route to be suppressed

display bgp routing-table different-origin-as

Syntax

display bgp routing-table different-origin-as

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table different-origin-as** command to display BGP routes originating from different autonomous systems.

Examples

Display BGP routes originating from different ASs.

```
<Sysname> display bgp routing-table different-origin-as
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  55.0.0.0         12.1.1.1       0                   0       100?
 *                   14.1.1.2       0                   0       300?
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table flap-info

Syntax

display bgp routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* } [**longer-match**]]]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: Displays route flap information that matches the AS path regular expression, which is a string of 1 to 80 characters.

as-path-acl-number: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-match: Matches the longest prefix.

Description

Use the **display bgp routing-table flap-info** command to display BGP route flap statistics.

Examples

Display BGP route flap statistics.

```
<Sysname> display bgp routing-table flap-info

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network        From        Flaps  Duration   Reuse     Path/Origin

 *>  55.0.0.0       12.1.1.1    2      00:00:16             100?
 *d  77.0.0.0       12.1.1.1    5      00:34:02   00:27:08  100?
```

Table 1-9 display bgp routing flap-info command output description

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Duration time of the flap route
Reuse	Reuse time of the route

Refer to Table 1-6 for description on the other fields above.

display bgp routing-table label

Syntax

display bgp routing-table label

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table label** command to display labeled BGP routing information.

Examples

Display labeled BGP routing information.

```
<Sysname> display bgp routing-table label

 BGP Local router ID is 6.6.6.7
 Status codes: * - valid, > - best, d - damped,
```

```
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 2


        Network             NextHop           In/Out Label

 *>     4.4.4.4/32          127.0.0.1         3/NULL
 *>     5.5.5.5/32          1.1.1.1           NULL/1024
```

The In/Out Label field refers to the inbound/outbound label. Refer to Table 1-6 for the description of other fields.

display bgp routing-table peer

Syntax

display bgp routing-table peer *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: IP address of a peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

statistic: Displays route statistics.

Description

Use the **display bgp routing-table peer** command to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

Examples

Display BGP routing information advertised to BGP peer 20.20.20.1.

```
<Sysname> display bgp routing-table peer 20.20.20.1 advertised-routes

 Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

*>  30.30.30.0/24     0.0.0.0        0                   0       i
*>  40.40.40.0/24     0.0.0.0        0                   0       i
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table regular-expression

Syntax

display bgp routing-table regular-expression *as-regular-expression*

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

Description

Use the **display bgp routing-table regular-expression** command to display BGP routing information matching the specified AS path regular expression.

Examples

Display BGP routing information matching AS path regular expression 300$.

```
<Sysname> display bgp routing-table regular-expression 300$

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
    Network           NextHop       MED        LocPrf    PrefVal Path/Ogn

*>  40.40.40.0/24     30.30.30.1    0                   0       300i
```

Refer to Table 1-6 for description on the fields above.

display bgp routing-table statistic

Syntax

display bgp routing-table statistic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp routing-table statistic** command to display BGP routing statistics.

Examples

Display BGP routing statistics.

```
<Sysname> display bgp routing-table statistic

 Total Number of Routes: 4
```

Table 1-10 display bgp routing-table statistic command output description

Field	Description
Total number of routes	Total number of routes

ebgp-interface-sensitive

Syntax

ebgp-interface-sensitive

undo ebgp-interface-sensitive

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **ebgp-interface-sensitive** command to enable the clearing of EBGP session on any interface that becomes down.

Use the undo **ebgp-interface-sensitive** command to disable the function.

This function is enabled by default.

Examples

In BGP view, enable the clearing of EBGP session on any interface that becomes down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ebgp-interface-sensitive
```

In BGP-VPN instance view, enable the clearing of EBGP session on any interface that becomes down (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] ebgp-interface-sensitive
```

filter-policy export (BGP/BGP-VPN instance view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing routing information, a string of 1 to 19 characters.

direct: Filters direct routes.

isis *process-id*: Filters outgoing routes redistributed from an ISIS process. The ID is in the range 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The ID is in the range 1 to 65535.

static: Filters static routes.

If no routing protocol is specified, all outgoing routes are filtered.

Description

Use the **filter-policy export** command to configure the filtering of outgoing routes.

Use the **undo filter-policy export** command to remove the filtering.

If no routing protocol is specified, all redistributed routes are filtered when advertised.

By default, the filtering is not configured.

Examples

In BGP view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

In BGP-VPN instance view, reference ACL 2000 to filter all outgoing routes (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 export
```

filter-policy import (BGP/BGP-VPN instance view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

Examples

In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 import
```

In BGP-VPN instance view, reference ACL 2000 to filter incoming routing information (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 import
```

graceful-restart (BGP view)

Syntax

graceful-restart

undo graceful-restart

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **graceful-restart** command to enable BGP Graceful Restart capability.

Use the **undo graceful-restart** command to disable BGP Graceful Restart capability.

By default, BGP Graceful Restart capability is disabled.

Note

During main and backup boards switchover, a GR-capable BGP speaker can maintain the packet forwarding table. During restart, it may not maintain the forwarding table.

Examples

Enable the Graceful Restart capability for BGP process 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart
```

graceful-restart timer restart

Syntax

graceful-restart timer restart *timer*

undo graceful-restart timer restart

View

BGP view

Default Level

2: System level

Parameters

timer: Maximum time for a peer to reestablish a BGP session, in the range 3 to 600 seconds.

Description

Use the **graceful-restart timer restart** command to configure the maximum time for a peer to reestablish a BGP session.

Use the **undo graceful-restart timer restart** command to restore the default.

By default, the maximum time for a peer to reestablish a BGP session is 150 seconds.

Examples

Configure the maximum time for a peer to reestablish a BGP session as 300 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer restart 300
```

graceful-restart timer wait-for-rib

Syntax

graceful-restart timer wait-for-rib *timer*

undo graceful-restart timer wait-for-rib

View

BGP view

Default Level

2: System level

Parameters

timer: Time to wait for the End-of-RIB marker, in the range 3 to 300 seconds.

Description

Use the **graceful-restart timer wait-for-rib** command to configure the time to wait for the End-of-RIB marker.

Use the **undo graceful-restart timer wait-for-rib** command to restore the default.

By default, the time to wait for the End-of-RIB marker is 180 seconds.

Note

- After a BGP session has been successfully (re)established, the End-of-RIB marker must be received within the time specified with this command.
- Using this command can speed up route convergence.

Examples

Set the time to wait for the End-of-RIB marker to 100 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer wait-for-rib 100
```

group (BGP/BGP-VPN instance view)

Syntax

group *group-name* [**external** | **internal**]

undo group *group-name*

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

external: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

internal: Creates an IBGP peer group; not supported in BGP-VPN instance view.

Description

Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

Examples

In BGP view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

In BGP-VPN instance view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 200
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
```

```
[Sysname-bgp-vpn1] peer 10.1.2.1 group test
```

import-route (BGP/BGP-VPN instance view)

Syntax

import-route *protocol* [*process-id* | **all-processes**] [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id* | **all-processes**]

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

protocol: Redistributes routes from the specified routing protocol, which can be **direct**, **isis**, **ospf**, **rip** or **static** at present.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **ospf**, or **rip**.

all-processes: Redistributes routes from all the processes of the specified protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

med-value: Specifies a MED value for redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description

Use the **import-route** command to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed with the **import-route** command is incomplete.

Examples

In BGP view, redistribute routes from RIP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] import-route rip
```

In BGP-VPN instance view, redistribute routes from RIP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] import-route rip
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **log-peer-change** command to enable the global BGP logging on peers going up and down.

Use the **undo log-peer-change** command to disable the function.

By default, the function is enabled.

Examples

Enable BGP logging on peers going up and down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] log-peer-change
```

network (BGP/BGP-VPN instance view)

Syntax

network *ip-address* [*mask* | *mask-length*] **route-policy** *route-policy-name*

undo network *ip-address* [*mask* | *mask-length*]

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

ip-address: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

route-policy-name: Routing policy applied to the route. The name is a string of 1 to 19 characters.

Description

Use the **network** command to inject a network to the local BGP routing table.

Use the **undo network** command to remove a network from the BGP routing table.

By default, no network route is injected.

Note that:

- The network route to be injected must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The ORIGIN attribute of the network route injected with the **network** command is IGP.

Examples

In BGP view, inject the network segment 10.0.0.0/16.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0
```

In BGP-VPN instance view, advertise the network segment 10.0.0.0/16 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0
```

network short-cut (BGP/BGP-VPN instance view)

Syntax

network *ip-address* [*mask* | *mask-length*] **short-cut**

undo network *ip-address* [*mask* | *mask-length*] **short-cut**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

ip-address: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description

Use the **network short-cut** command to configure an eBGP route as a shortcut route.

Use the **undo network short-cut** command to restore the default.

By default, a received eBGP route has a priority of 255.

The **network short-cut** command allows you configure an eBGP route as a shortcut route that has the same priority as a local route and thus has greater likehood to become the optimal route.

Examples

In BGP view, configure route 10.0.0.0/16 as a shortcut route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0 short-cut
```

In BGP-VPN instance view, configure route 10.0.0.0/16 as a shortcut route. (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0 short-cut
```

peer advertise-community (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list, if-match community**, **apply community** (refer to *Routing Policy Commands* in the *IP Routing Volume*).

Examples

In BGP view, advertise the community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

In BGP-VPN instance view, advertise the community attribute to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer advertise-ext-community (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **advertise-ext-community**

undo peer { *group-name* | *ip-address* } **advertise-ext-community**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the extended community attribute advertisement to a peer/peer group.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to the **ip extcommunity-list**, **if-match extcommunity** and **apply extcommunity** commands in *Routing Policy Commands* of the *IP Routing Volume*.

Examples

In BGP view, advertise the extended community attribute to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

In BGP-VPN view, advertise the extended community attribute to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer allow-as-loop (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

number: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the number of times the local AS number can appear.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is not allowed in routes from a peer/peer group.

Related commands: display bgp routing-table peer.

Examples

In BGP view, configure the number of times the local AS number can appear in AS-path attribute of routes from peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

In BGP-VPN instance view, configure the number of times for which the local AS number can appear in AS-path attribute of routes from peer 1.1.1.1 as 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

peer as-number (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **as-number** *as-number*

undo peer *group-name* **as-number**

undo peer *ip-address*

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer or peer group, in the range 1 to 65535.

Description

Use the **peer as-number** command to specify a peer/peer group with an AS number.

Use the **undo peer as-number** command to delete a peer group.

Use the **undo peer** command to delete a peer.

By default, no peer or peer group is specified.

You can specify the AS number of a peer in either of the following two ways:

- Use the **peer** *ip-address* **as-number** *as-number* command. After that, the system creates the specified peer by default.
- Specify the AS number of the peer when adding it to the specified peer group by using the **peer** *ip-address* **group** *group-name* **as-number** *as-number* command; or use the **peer as-number** command to specify the AS number of a peer group, and then a newly added peer will belong to the AS.

The AS number of a peer/peer group cannot be modified directly. To do so, you have to delete the peer/peer group and configure it again.

Examples

In BGP view, specify peer group **test** in AS 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
```

In BGP-VPN instance view, specify peer group **test2** in AS 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test2 as-number 200
```

peer as-path-acl (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-path-acl-number: AS path ACL number, in the range 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Description

Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL filtering is configured.

Related commands: **ip as-path**, **if-match as-path** and **apply as-path** (refer to *IP Routing Policy Commands* in the *IP Routing Volume*).

Examples

In BGP view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export
```

In BGP-VPN instance view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-path-acl 1 export
```

peer capability-advertise conventional

Syntax

peer { *group-name* | *ip-address* } **capability-advertise conventional**

undo peer { *group-name* | *ip-address* } **capability-advertise conventional**

View

BGP view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer capability-advertise conventional** command to disable BGP multi-protocol extension and route refresh for a peer/peer group.

Use the **undo peer capability-advertise** command to enable BGP multi-protocol extension and route refresh for a peer/peer group.

By default, BGP multi-protocol extension and route refresh are enabled.

Examples

In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

peer capability-advertise route-refresh

Syntax

peer { *group-name* | *ip-address* } **capability-advertise route-refresh**

undo peer { *group-name* | *ip-address* } **capability-advertise route-refresh**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer capability-advertise route-refresh** command to enable the BGP route refresh capability.

Use the **undo peer capability-advertise route-refresh** command to disable the capability.

The capability is enabled by default.

Examples

In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

In BGP-VPN instance view, enable BGP route refresh for peer 160.89.2.33 (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 160.89.2.33 as-number 200
[Sysname-bgp-vpn1] peer 160.89.2.33 capability-advertise route-refresh
```

peer connect-interface (BGP/BGP-VPN instance view)

Syntax

peer { group-name | ip-address } **connect-interface** interface-type interface-number

undo peer { *group-name* | *ip-address* } **connect-interface**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string 1 to 47 characters.

ip-address: IP address of a peer.

interface-type interface-number: Specifies the type and number of the interface.

Description

Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to a peer/peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the BGP peer/peer group as the source interface for establishing a TCP connection to the peer/peer group.

Note that:

To establish multiple BGP connections to another BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples

In BGP view, specify loopback 0 as the source interface for routing updates to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test connect-interface loopback 0
```

In BGP-VPN instance view, specify loopback 0 as the source interface for routing updates to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-vpn1] peer test connect-interface loopback 0
```

peer default-route-advertise (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ip-address* } **default-route-advertise**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples

In BGP view, advertise a default route to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise
```

In BGP-VPN instance view, advertise a default route to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test default-route-advertise
```

peer description (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **description** *description-text*

undo peer { *group-name* | *ip-address* } **description**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description

Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

Examples

In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

In BGP-VPN instance view, configure the description information of the peer group test as ISP1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test description ISP1
```

peer ebgp-max-hop (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ip-address* } **ebgp-max-hop**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

hop-count: Maximum hop count, in the range 1 to 255. The default is 64.

Description

Use the **peer ebgp-max-hop** command to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.

Use the **undo peer ebgp-max-hop** command to restore the default.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum route hop count of the EBGP connection.

Examples

In BGP view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ebgp-max-hop
```

In BGP-VPN instance view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ebgp-max-hop
```

peer enable (BGP view)

Syntax

peer *ip-address* **enable**

undo peer *ip-address* **enable**

View

BGP view

Default Level

2: System level

Parameters

ip-address: IP address of a peer.

Description

Use the **peer enable** command to enable the specified peer.

Use the **undo peer enable** command to disable the specified peer.

By default, the BGP peer is enabled.

If a peer is disabled, the router will not exchange routing information with the peer.

Examples

Disable peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 group group1
[Sysname-bgp] undo peer 18.10.0.9 enable
```

peer fake-as (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **fake-as** *as-number*

undo peer { *group-name* | *ip-address* } **fake-as**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description

Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Note

The **peer fake-as** command is only applicable to an EBGP peer or peer group.

Examples

In BGP view, configure a fake AS number of 200 for the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test fake-as 200
```

In BGP-VPN instance view, configure a fake AS number of 200 for the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test fake-as 200
```

peer filter-policy (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** [*acl-number*] { **export** | **import** }

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Applies the filter-policy to routes advertised to the peer/peer group.

import: Applies the filter-policy to routes received from the peer/peer group.

Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

Examples

In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

In BGP-VPN instance view, apply the ACL 2000 to filter routes advertised to the peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test filter-policy 2000 export
```

peer group (BGP/BGP-VPN instance view)

Syntax

peer *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer, in the range 1 to 65535.

Description

Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

If you have specified an AS number for the peer to be added, make sure that the *as-number* argument is consistent with the specified peer AS number.

If you have not created the peer to be added, the system automatically creates the peer when you execute the command.

Examples

In BGP view, add the peer 10.1.1.1 to the EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

In BGP-VPN view, add the peer 10.1.1.1 to the EBGP peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 2004
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
```

peer ignore (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **ignore**

undo peer { *group-name* | *ip-address* } **ignore**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer ignore** command to disable session establishment with a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, session establishment with a peer or peer group is allowed.

After the **peer ignore** command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, this means all sessions with the peer group will be tore down.

Examples

In BGP view, disable session establishment with peer 10.10.10.10.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.10.10.10 ignore
```

In BGP-VPN instance view, disable session establishment with peer 10.10.10.10 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.10.10.10 ignore
```

peer ip-prefix

Syntax

peer { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Description

Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list based filtering is configured.

Examples

In BGP view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export
```

In BGP-VPN view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ip-prefix list1 export
```

peer keep-all-routes (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **keep-all-routes**

undo peer { *group-name* | *ip-address* } **keep-all-routes**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, including routes that fail to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples

In BGP view, save routing information from peer 131.100.1.1.

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

```
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes
```

In BGP-VPN instance view, save routing information from peer 131.100.1.1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.100.1.1 as-number 200
[Sysname-bgp-vpn1] peer 131.100.1.1 keep-all-routes
```

peer log-change (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **log-change**

undo peer { *group-name* | *ip-address* } **log-change**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer log-change** command to enable the logging of session state and event information for a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples

In BGP view, enable the logging of session state and event information for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

In BGP-VPN instance view, enable the logging of session state and event information for peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test log-change
```

peer next-hop-local (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View

BGP view /BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer next-hop-local** command to specify the router as the next hop for routes sent to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes sent to an IBGP peer/peer group do not take the local router as the next hop.

Examples

In BGP view, set the next hop of routes advertised to peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

In BGP-VPN instance view, set the next hop of routes advertised to peer group **test** to the router itself (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test next-hop-local
```

peer password

Syntax

peer { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*

undo peer { group-name | ip-address } **password**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

cipher: Displays the configured password in cipher text format.

simple: Displays the configured password in plain text format.

password: Password, a string of 1 to 80 characters when the **simple** keyword is used, or when the **cipher** keyword and plain text password are used; a string of 24 or 108 characters when the cipher text password and the **cipher** keyword are used.

Description

Use the **peer password** command to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use the **undo peer password** command to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

Examples

In BGP view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

In BGP-VPN instance view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 200
[Sysname-bgp-vpn1] peer 10.1.100.1 password simple aabbcc
```

peer preferred-value (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

value: Preferred value, in the range 0 to 65535.

Description

Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value. Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the route to the destination.

Note that:

If you both reference a routing policy and use the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command to set a preferred value for routes from a peer, the routing policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value specified in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the command **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** } in this document, and the command **apply preferred-value** *preferred-value* in *Routing Policy Commands* of the *IP Routing Volume*.

Examples

In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

In BGP-VPN instance view, configure the preferred value as 50 for routes from peer 131.108.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-vpn1] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

Examples

In BGP view, carry no private AS number in BGP updates sent to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

In BGP-VPN instance view, carry no private AS number in BGP updates sent to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test public-as-only
```

peer reflect-client (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View

BGP view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither the route reflector nor the client is configured.

Related commands: **reflect between-clients** and **reflect cluster-id**.

Examples

In BGP view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

peer route-limit (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **route-limit** *prefix-number* [{ **alert-only** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ip-address* } **route-limit**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

prefix-number: Number of prefixes that can be received from the peer or peer group, in the range 1 to 128000. If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will tear down the connection to the peer/peer group.

alert-only: If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will not tear down the connection to the peer/peer group but display an alarm message.

reconnect *reconnect-time:* Specifies a reconnect time, after which, the router will re-establish a connection to the peer/peer group. It has no default value and is in the range 1 to 65535 seconds.

percentage-value: Threshold value for the router to display an alarm message (that is, the router displays an alarm message when the ratio of the number of received prefixes to the *prefix-number* reaches the *percentage*). It is in the range 1 to 100 and defaults to 75.

Description

Use the **peer route-limit** command to set the number of route prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is not limited by default.

Examples

In BGP view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

In BGP-VPN instance view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 129.140.6.6 as-number 110
[Sysname-bgp-vpn1] peer 129.140.6.6 route-limit 10000
```

peer route-policy (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

export: Applies the routing policy to routes outgoing to the peer (or peer group).

import: Applies the routing policy to routes incoming from the peer (or peer group).

Description

Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is applied to routes from/to the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. Refer to *Routing Policy Commands* in the *IP Routing Volume* for related commands.

Examples

In BGP view, apply routing policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

In BGP-VPN instance view, apply the routing policy **test-policy** to routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test route-policy test-policy export
```

peer route-update-interval (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **route-update-interval** *interval*

undo peer { *group-name* | *ip-address* } **route-update-interval**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

interval: Minimum interval for sending the same update message. The range is 5 to 600 seconds.

Description

Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default value.

By default, the interval is 15 seconds for IBGP peers, and 30 seconds for EBGP peers.

Examples

In BGP view, specify the interval for sending the same update to peer group **test** as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

In BGP-VPN instance view, specify the interval for sending the same update to peer group **test** as 10 seconds (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
[Sysname-bgp-vpn1] peer test route-update-interval 10
```

peer substitute-as (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **substitute-as**

undo peer { *group-name* | *ip-address* } **substitute-as**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use the **peer substitute-as** command to replace the AS number of a peer/peer group in the AS_PATH attribute with the local AS number.

Use the **undo peer substitute-as** command to remove the configuration.

No AS number is replaced by default.

Examples

In BGP view, substitute local AS number for AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 substitute-as
```

In BGP-VPN instance view, substitute local AS number for AS number of peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 substitute-as
```

peer timer (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ip-address* } **timer**

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

keepalive: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description

Use the **peer timer** command to configure the keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s respectively.

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples

In BGP view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test timer keepalive 60 hold 180
```

preference (BGP/BGP-VPN instance view)

Syntax

preference { *external-preference* *internal-preference* *local-preference* | **route-policy** *route-policy-name* }

undo preference

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

external-preference: Preference of EBGP routes, in the range 1 to 255.

internal-preference: Preference of IBGP routes, in the range 1 to 255.

local-preference: Preference of local routes, in the range 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. Using the routing policy can set a preference for routes matching it. The default value applies to routes not matching the routing policy.

Description

Use the **preference** command to configure preferences for external, internal, and local routes.

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

For *external-preference*, *internal-preference* and *local-preference*, the greater the preference value is, the lower the preference is, and the default values are 255, 255, 130 respectively.

Examples

In BGP view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] preference 20 20 200
```

In BGP-VPN instance view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] preference 20 20 200
```

reflect between-clients (BGP view)

Syntax

reflect between-clients

undo reflect between-clients

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples

Disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients
```

reflector cluster-id (BGP view)

Syntax

reflector cluster-id { *cluster-id* | *ip-address* }

undo reflector cluster-id

View

BGP view

Default Level

2: System level

Parameters

cluster-id: Cluster ID in the format of an integer from 1 to 4294967295.

ip-address: Cluster ID in the format of an IPv4 address in dotted decimal notation.

Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. In this case, using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples

Set the cluster ID to 80.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80
```

refresh bgp

Syntax

refresh bgp { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

all: Soft-resets all BGP connections.

ip-address: Soft-resets the BGP connection to a peer.

group-name: Soft-resets connections to a peer group, name of which is a sting of 1 to 47 characters.

external: EBGP connection.

internal: IBGP connection.

export: Outbound soft reset.

import: Inbound soft reset.

Description

Use the **refresh bgp** command to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all routers in the network must support route-refresh. If a router not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

Examples

Perform inbound BGP soft reset.

```
<Sysname> refresh bgp all import
```

reset bgp

Syntax

reset bgp { **all** | *as-number* | *ip-address* [**flap-info**] | **group** *group-name* | **external** | **internal** }

View

User view

Default Level

1: Monitor level

Parameters

all: Resets all BGP connections.

as-number: Resets BGP connections to peers in the AS.

ip-address: Specifies the IP address of a peer with which to reset the connection.

flap-info: Clears routing flap information.

group *group-name*: Resets connections with the specified BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description

Use the **reset bgp** command to reset specified BGP connections.

Examples

Reset all the BGP connections.

```
<Sysname> reset bgp all
```

reset bgp dampening

Syntax

reset bgp dampening [*ip-address* [*mask* | *mask-length*]]

View

User view

Default Level

1: Monitor level

Parameters

ip-address: Destination IP address of a route.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description

Use the **reset bgp dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening**, **display bgp routing-table dampened**.

Examples

Clear damping information of route 20.1.0.0/16 and release the suppressed route.

```
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

reset bgp flap-info

Syntax

reset bgp flap-info [**regexp** *as-path-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]

View

User view

Default Level

1: Monitor level

Parameters

as-path-regular-expression: Clears the flap statistics of routes matching the AS path regular expression, which is a string of 1 to 80 characters.

as-path-acl-number: Clears the flap statistics of routes matching an AS path ACL, number of which is in the range 1 to 256.

ip-address: Clears the flap statistics of a route.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description

Use the **reset bgp flap-info** command to clear the flap statistics of routes matching the specified filter.

Examples

Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp flap-info as-path-acl 10
```

reset bgp ipv4 all

Syntax

reset bgp ipv4 all

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **reset bgp ipv4 all** command to reset all the BGP connections of IPv4 unicast address family.

Examples

Reset all the BGP connections of IPv4 unicast address family.

```
<Sysname> reset bgp ipv4 all
```

router-id

Syntax

router-id *router-id*

undo router-id

View

BGP view

Default Level

2: System level

Parameters

router-id: Router ID in IP address format.

Description

Use the **router-id** command to specify a router ID.

Use the **undo router-id** command to remove the router ID.

To run BGP protocol, a router must have a router ID, which is an unsigned 32-bit integer, the unique ID of the router in the AS.

You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is the highest IP address among loopback interface addresses; if not available, then the highest IP address of interfaces. It is recommended to specify a loopback interface address as the router ID to enhance network reliability.

Only when the interface with the selected Router ID or the manual Router ID is deleted will the system select another ID for the router.

Examples

Specifies the Router ID as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

summary automatic

Syntax

summary automatic

undo summary automatic

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- Neither the default route nor the routes imported using the **network** command can be summarized automatically.
- The **summary automatic** command helps BGP limit the number of routes redistributed from IGP to reduce the size of the routing table.

Examples

In BGP view, enable automatic route summarization.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic
```

In BGP-VPN instance view, enable automatic summarization (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] summary automatic
```

synchronization (BGP view)

Syntax

synchronization

undo synchronization

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **synchronization** command to enable the synchronization between the BGP and IGP routes.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

When a BGP router receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

Examples

Enable the synchronization between BGP and IGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] synchronization
```

timer (BGP/BGP-VPN instance view)

Syntax

timer keepalive *keepalive* **hold** *holdtime*

undo timer

View

BGP view/BGP-VPN instance view

Default Level

2: System level

Parameters

keepalive: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description

Use the **timer** command to configure BGP keepalive interval and holdtime interval.

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

By default, BGP keepalive and holdtime intervals are 60s and 180s.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using this command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the BGP peers, while it becomes valid only after the corresponding BGP connections are reset.

Related commands: **peer timer**.

Examples

Configure keepalive interval and holdtime interval as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure keepalive interval and holdtime interval as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] timer keepalive 60 hold 180
```

Table of Contents

1 IPv6 Static Routing Configuration Commands

Note

- Throughout this chapter, the term “router” refers to a router in a generic sense or a Layer 3 switch running routing protocols.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

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 IPv6 RIPng Configuration Commands

Note

- The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

RIPng Configuration Commands

checkzero

Syntax

checkzero

undo checkzero

View

RIPng view

Default Level

2: System level

Parameters

None

Description

Use the **checkzero** command to enable the zero field check on RIPng packets.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

Examples

Disable the zero field check on RIPng packet headers of RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

default cost (RIPng view)

Syntax

default cost *cost*

undo default cost

View

RIPng view

Default Level

2: System level

Parameters

cost: Default metric of redistributed routes, in the range of 0 to 16.

Description

Use the **default cost** command to specify the default metric of redistributed routes.

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

The default metric of redistributed routes is 0.

The specified default metric applies to the routes redistributed by the **import-route** command with no metric specified.

Related commands: **import-route**.

Examples

Set the default metric of redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

display ripng

Syntax

display ripng [*process-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use the **display ripng** command to display the running status and configuration information of a RIPng process. If *process-id* is not specified, information of all RIPng processes will be displayed.

Examples

Display the running status and configuration information of all configured RIPng processes.

```
<Sysname> display ripng
    RIPng process : 1
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 3
       Update time     :   30 sec(s)  Timeout time           :  180 sec(s)
       Suppress time   :  120 sec(s)  Garbage-Collect time :  240 sec(s)
       Number of periodic updates sent : 0
       Number of trigger updates sent : 0
```

Table 1-1 display ripng command output description

Field	Description
RIPng process	RIPng process ID
Preference	RIPng route priority
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled
Default Cost	Default metric of redistributed routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIPng update interval, in seconds
Timeout time	RIPng timeout interval, in seconds
Suppress time	RIPng suppress interval, in seconds
Garbage-Collect time	RIPng garbage collection interval, in seconds
Number of periodic updates sent	Number of periodic updates sent
Number of trigger updates sent	Number of triggered updates sent

display ripng database

Syntax

display ripng *process-id* **database**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use the **display ripng database** command to display all active routes in the RIPng advertising database, which are sent in normal RIPng update messages.

Examples

Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
   2001:7B::2:2A1:5DE/64,
        cost 4, Imported
   1:13::/120,
        cost 4, Imported
   1:32::/120,
        cost 4, Imported
   1:33::/120,
        cost 4, Imported
   100::/32,
       via FE80::200:5EFF:FE04:3302, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   3FFE:C00:C18:2::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:3::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   4000:1::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
   4000:2::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
   1111::/64,
        cost 0, RIPng-interface
```

Table 1-2 display ripng database command output description

Field	Description
2001:7B::2:2A1:5DE/64	IPv6 destination address/prefix length
via	Next hop IPv6 address
cost	Route metric value
Imported	Route redistributed from another routing protocol
RIPng-interface	Route learned from the interface

display ripng interface

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface.

Description

Use the **display ripng interface** command to display the interface information of the RIPng process.

If no interface is specified, information about all interfaces of the RIPng process will be displayed.

Examples

Display the interface information of RIPng process 1.

```
<Sysname> display ripng 1 interface
Interface-name: Vlan-interface100
          Link Local Address: FE80::20F:E2FF:FE30:C16C
          Split-horizon: on                Poison-reverse: off
          MetricIn: 0                      MetricOut: 1
          Default route: off
          Summary address:
                 3:: 64
                 3:: 16
```

Table 1-3 display ripng interface command output description

Field	Description
Interface-name	Name of an interface running RIPng
Link Local Address	Link-local address of an interface running RIPng
Split-horizon	Indicates whether the split horizon function is enabled (on: Enabled; off: Disabled)
Poison-reverse	Indicates whether the poison reverse function is enabled (on: Enabled; off: Disabled)
MetricIn/MetricOut	Additional metric to incoming and outgoing routes
Default route	• Only/Originate: **Only** means that the interface advertises only the default route. **Originate** means that the default route and other RIPng routes are advertised. • **Off** indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled. • In garbage-collect status: With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time.
Summary address	The summarized IPv6 prefix and the summary IPv6 prefix on the interface

display ripng route

Syntax

display ripng *process-id* **route**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use the **display ripng route** command to display all RIPng routes and timers associated with each route of a RIPng process.

Examples

Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::200:5EFF:FE04:B602  on Vlan-interface100
 Dest 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec

 Dest 3FFE:C00:C18:2::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec
```

Table 1-4 display ripng route command output description

Field	Description
Peer	Neighbor connected to the interface
Dest	IPv6 destination address
via	Next hop IPv6 address
cost	Routing metric value
tag	Route tag
Sec	Time that a route entry stays in a particular state
“A”	The route is in the aging state.
“S”	The route is in the suppressed state.
“G”	The route is in the Garbage-collect state.

filter-policy export

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View

RIPng view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of an ACL to filter advertised routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter routing information, a string of 1 to 19 characters.

protocol: Filters routes redistributed from a routing protocol, currently including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**.

process-id: Process number of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **rip**, **ospf**, or **isis**.

Description

Use the **filter-policy export** command to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use the **undo filter-policy export** command to restore the default.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all outgoing routing information will be filtered.

Examples

Use IPv6 prefix list **Filter 2** to filter advertised RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

filter-policy import (RIPng view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View

RIPng view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of an ACL to filter incoming routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list to filter incoming routes, in the range 1 to 19 characters.

Description

Use the **filter-policy import** command to define an inbound route filtering policy. Only routes which match the filtering policy can be received.

Use the **undo filter-policy import** command to disable inbound route filtering.

By default, RIPng does not filter incoming routing information.

Examples

Reference IPv6 prefix list **Filter1** to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

import-route

Syntax

import-route *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View

RIPng view

Default Level

2: System level

Parameters

protocol: Specifies a routing protocol from which to redistribute routes. Currently, it can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1.This argument is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

cost: Routing metric of redistributed routes, in the range of 0 to 16. If *cost value* is not specified, the metric is the default metric specified by the **default cost** command.

route-policy *route-policy-name*: Specifies a routing policy by its name with 1 to 19 characters.

allow-ibgp: Optional keyword when the specified *protocol* is **bgp4+**. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes, thus be cautious when using it.

Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

- You can configure a routing policy to redistribute only needed routes.
- You can specify a cost for redistributed routes using the **cost** keyword.

Related commands: **default cost**.

Examples

Redistribute IPv6-IS-IS routes (process 7) and specify the metric as 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing (RIPng view)

Syntax

maximum load-balancing *number*

undo maximum load-balancing

View

RIPng view

Default Level

2: System level

Parameters

number: Maximum number of equal-cost load-balanced routes. Its value is in the range 1 to 4.

Description

Use the **maximum load-balancing** command to specify the maximum number of equal-cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes for load balancing is 4.

Note

Configure the maximum number according to the memory size.

Examples

Set the maximum number of load balanced routes with equal cost to 2.

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

```
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-ripng-100] undo maximum load-balancing
```

preference

Syntax

preference [**route-policy** *route-policy-name*] *preference*

undo preference [**route-policy**]

View

RIPng view

Default Level

2: System level

Parameters

route-policy-name: Name of a routing policy, in the range of 1 to 19 characters.

preference: RIPng route priority, in the range of 1 to 255.

Description

Use the **preference** command to specify the RIPng route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIPng route is 100.

Using the **route-policy** keyword can set a priority for routes filtered in by the routing policy:

- If a priority is set in the routing policy, the priority applies to matched routes, and the priority set by the **preference** command applies to routes not matched.
- If no priority is set in the routing policy, the one set by the **preference** command applies to all routes.

Examples

Set the RIPng route priority to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

Restore the default RIPng route priority.

```
[Sysname-ripng-100] undo preference
```

ripng

Syntax

ripng [*process-id*]

undo ripng [*process-id*]

View

System view

Default Level

2: System level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535. The default value is 1.

Description

Use the **ripng** command to create a RIPng process and enter RIPng view.

Use the **undo ripng** command to disable a RIPng process.

By default, no RIPng process is enabled.

Examples

Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

Disable RIPng process 100.

```
[Sysname] undo ripng 100
```

ripng default-route

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

View

Interface view

Default Level

2: System level

Parameters

only: Indicates that only the IPv6 default route (::/0) is advertised through the interface.

originate: Indicates that the IPv6 default route (::/0) is advertised without suppressing other routes.

cost: Metric of the advertised default route, in the range of 1 to 15, with a default value of 1.

Description

Use the **ripng default-route** command to advertise a default route with the specified routing metric to a RIPng neighbor.

Use the **undo ripng default-route** command to stop advertising or forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in the local IPv6 routing table.

Examples

Advertise only the default route through VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

Advertise the default route together with other routes through VLAN-interface 101.

```
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Syntax

ripng *process-id* **enable**

undo ripng enable

View

Interface view

Default Level

2: System level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use the **ripng enable** command to enable RIPng on the specified interface.

Use the **undo ripng enable** command to disable RIPng on the specified interface.

By default, RIPng is disabled on an interface.

Examples

Enable RIPng100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng metricin

Syntax

ripng metricin *value*

undo ripng metricin

View

Interface view

Default Level

2: System level

Parameters

value: Additional metric for received routes, in the range of 0 to 16.

Description

Use the **ripng metricin** command to specify an additional metric for received RIPng routes.

Use the **undo ripng metricin** command to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout**.

Examples

Specify the additional routing metric as 12 for RIPng routes received by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Syntax

ripng metricout *value*

undo ripng metricout

View

Interface view

Default Level

2: System level

Parameters

value: Additional metric to advertised routes, in the range of 1 to 16.

Description

Use the **ripng metricout** command to configure an additional metric for RIPng routes advertised by an interface.

Use the **undo rip metricout** command to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin**.

Examples

Set the additional metric to 12 for routes advertised by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng poison-reverse

Syntax

ripng poison-reverse

undo ripng poison-reverse

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples

Enable the poison reverse function for RIPng update messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse
```

ripng split-horizon

Syntax

ripng split-horizon

undo ripng split-horizon

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

By default, the split horizon function is enabled.

Note that:

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure that it is necessary to disable the split horizon function before doing so.

 **Note**

If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.

Examples

Enable the split horizon function on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

View

Interface view

Default Level

2: System level

Parameters

ipv6-address: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Description

Use the **ripng summary-address** command to configure a summary advertised through the interface.

Use the **undo ripng summary-address** command to remove the summary.

If the prefix and the prefix length of a route match the IPv6 prefix, the IPv6 prefix will be advertised instead. Thus, one route can be advertised on behalf of many routes. After summarization, the summary route cost is the lowest cost among summarized routes.

Examples

Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix length.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

timers

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View

RIPng view

Default Level

2: System level

Parameters

garbage-collect-value: Interval of the garbage-collect timer in seconds, in the range of 1 to 86400.

suppress-value: Interval of the suppress timer in seconds, in the range of 0 to 86400.

timeout-value: Interval of the timeout timer in seconds, in the range of 1 to 86400.

update-value: Interval of the update timer in seconds, in the range of 1 to 86400.

Description

Use the **timers** command to configure RIPng timers.

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

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the above four timers.

- The update timer defines the interval between update messages.
- The timeout timer defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines for how long a RIPng route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.

- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with the routing metric set to 16. If no update message is announced for that route before the garbage-collect timer expires, the route will be completely deleted from the routing table.

Note that:

- You are not recommended to change the default values of these timers under normal circumstances.
- The lengths of these timers must be kept consistent on all routers and access servers in the network

Examples

Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

Table of Contents

1 IPv6 OSPFv3 Configuration Commands

Note

- The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

OSPFv3 Configuration Commands

abr-summary (OSPFv3 area view)

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**]

undo abr-summary *ipv6-address prefix-length*

View

OSPFv3 area view

Default Level

2: System level

Parameters

ipv6-address: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address, in the range 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route.

Description

Use the **abr-summary** command to configure an IPv6 summary route on an area border router.

Use the **undo abr-summary** command to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is available on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

Examples

Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area (OSPFv3 view)

Syntax

area *area-id*

View

OSPFv3 view

Default Level

2: System level

Parameters

area-id: ID of an area, a decimal integer (in the range of 0 to 4294967295 and changed to IPv4 address format by the system) or an IPv4 address.

Description

Use the **area** command to enter OSPFv3 area view.

Note

The undo form of the command is not available. An area is removed automatically if there is no configuration and no interface is up in the area.

Examples

Enter OSPFv3 Area 0 view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

bandwidth-reference

Syntax

bandwidth-reference *value*

undo bandwidth-reference

View

OSPFv3 view

Default Level

2: System level

Parameters

value: Bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

Description

Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

You can configure an OSPFv3 cost for an interface with one of the following two methods:

- Configure the cost value in interface view.
- Configure a bandwidth reference value, and OSPFv3 computes the cost automatically based on the bandwidth reference value: Interface OSPFv3 cost = Bandwidth reference value/Interface bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically:

Examples

Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] bandwidth-reference 1000
```

default cost

Syntax

default cost *value*

undo default cost

View

OSPFv3 view

Default Level

2: System level

Parameters

value: Specifies a default cost for redistributed routes, in the range of 1 to 16777214.

Description

Use the **default cost** command to configure a default cost for redistributed routes.

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

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

If multiple OSPFv3 processes are available, use of this command takes effect for the current process only.

Examples

Specify the default cost for redistributed routes as 10.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default cost 10
```

default-cost (OSPFv3 area view)

Syntax

default-cost *value*

undo default-cost

View

OSPFv3 area view

Default Level

2: System level

Parameters

value: Specifies a cost for the default route advertised to the stub area, in the range of 0 to 65535. The default is 1.

Description

Use the **default-cost** command to specify the cost of the default route to be advertised to the stub area.

Use the **undo-default-cost** command to restore the default value.

Use of this command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

If multiple OSPFv3 processes are running, use of this command takes effect only for the current process.

Related commands: **stub**.

Examples

Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

default-route-advertise

Syntax

default-route-advertise [**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] *

undo default-route-advertise

View

OSPFv3 view

Default Level

2: System level

Parameters

always: Generates a default route in an ASE LSA into the OSPF routing domain regardless of whether the default route exists in the routing table. Without this keyword, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain only when the default route exists in the routing table.

cost *cost*: Specifies a cost for the default route, in the range 0 to 16777214. The default is 1.

type *type*: Specifies a type for the ASE LSA: 1 or 2. The default is 2.

route-policy *route-policy-name*: Specifies a route policy name, a string of 1 to 19 characters.

Description

Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from redistributing a default route.

By default, no default route is redistributed.

Using the **import-route** command cannot redistribute a default route. To do so, you need to use the **default-route-advertise** command. If no default route exists in the router's routing table, use the **default-route-advertise always** command to generate a default route in a Type-5 LSA.

You can reference a routing policy to set the cost and type of the default route:

- The router advertises the default route only when it passes the routing policy.
- The default route passing the routing policy uses the cost set by the **apply cost** clause, and the type set by the **apply cost-type** clause in the routing policy.
- The default route cost's priority from high to low is: the cost set by the **apply cost** clause in the routing policy, the one set by the **default-route-advertise** command and the one set by the **default cost** command.
- The default route type's priority from high to low is: the type set by the **apply cost-type** clause in the routing policy, and the one set by the **default-route-advertise** command.
- If the **always** keyword is included, the default route is advertised regardless of whether it passes the routing policy and uses the cost and type specified by the **apply cost**, **apply cost-type** clauses in the first node of the routing policy.

Related commands: **import-route**.

Examples

Generate a default route into the OSPFv3 routing domain.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

display ospfv3

Syntax

display ospfv3 [*process-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

Description

Use the **display ospfv3** command to display the brief information of an OSPFv3 process. If no process ID is specified, OSPFv3 brief information about all processes will be displayed.

Examples

Display brief information about all OSPFv3 processes.

```
<Sysname> display ospfv3
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. These external LSAs’ checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 3
 Number of LSA received 0
 Number of areas in this router is 1
  Area 0.0.0.1
       Number of interfaces in this area is 1
       SPF algorithm executed 1 times
       Number of LSA 2. These LSAs’ checksum Sum 0x20C8
       Number of Unknown LSA 0
```

Table 1-1 display ospfv3 command output description

Field	Description
Routing Process "OSPFv3 (1)" with ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
SPF schedule delay	Delay interval of SPF calculation
Hold time between SPFs	Hold time between SPF calculations
Minimum LSA interval	Minimum interval for generating LSAs
Minimum LSA arrival	Minimum LSA repeat arrival interval

Field	Description
Number of external LSA	Number of ASE LSAs
These external LSAs' checksum Sum	Sum of all the ASE LSAs' checksum
Number of AS-Scoped Unknown LSA	Number of LSAs with unknown flooding scope
Number of LSA originated	Number of LSAs originated
Number of LSA received	Number of LSAs received
Number of areas in this router	Number of areas this router is attached to
Area	Area ID
Number of interfaces in this area	Number of interfaces attached to this area
SPF algorithm executed 1 times	SPF algorithm is executed 1 time
Number of LSA	Number of LSAs
These LSAs' checksum Sum	Sum of all LSAs' checksum
Number of Unknown LSA	Number of unknown LSAs

display ospfv3 interface

Syntax

display ospfv3 interface [*interface-type interface-number* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

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

statistic: Displays the interface statistics.

Description

Use the **display ospfv3 interface** command to display OSPFv3 interface information.

Examples

Display OSPFv3 interface information.

```
<Sysname> display ospfv3 interface vlan-interface 100
Vlan-interface100 is up, line protocol is up
  Interface ID 2320063
  IPv6 Prefixes
    FE80::200:FCFF:FE00:6505 (Link-Local Address)
    1::1
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID: 1.1.1.1, Network Type: BROADCAST, Cost: 1
```

```
Transmit Delay is 1 sec, State: Waiting, Priority: 1
No designated router on this link
No backup designated router on this link
Timer interval configured
  Hello: 10, Dead: 40, Poll: 40, Wait: 40, Retransmit: 5
  Hello due in 00:00:05
Neighbor Count is 0, Adjacent neighbor count is 0
```

Table 1-2 display ospfv3 interface command output description

Field	Description
Interface ID	Interface ID
IPv6 Prefixes	IPv6 Prefix
OSPFv3 Process	OSPFv3 Process
Area	Area ID
Instance ID	Instance ID
Router ID	Router ID
Network Type	Network type of the interface
Cost	Cost value of the interface
Transmit Delay	Transmission delay of the interface
State	Interface state
Priority	DR priority of the interface
No designated router on this link	No designated router on this link
No backup designated router on this link	No backup designated router on this link
Timer interval configured, Hello: 10, Dead: 40, Poll: 40, Wait: 40, Retransmit: 5	Time intervals in seconds configured on the interface, Hello: 10, Dead: 40, Poll: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Hello packet will be sent in 2 seconds
Neighbor Count	Number of Neighbors on the interface
Adjacent neighbor count	Number of Adjacencies on the interface

display ospfv3 lsdb

Syntax

display ospfv3 [*process-id*] **lsdb** [[**external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router**] [*link-state-id*] [**originate-router** *router-id*] | **total**]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

external: Displays information about AS-external LSAs.

inter-prefix: Displays information about Inter-area-prefix LSAs.

inter-router: Displays information about Inter-area-router LSAs.

intra-prefix: Displays information about Intra-area-prefix LSAs.

link: Displays information about Link-LSAs.

network: Displays information about Network-LSAs.

router: Displays information about Router-LSAs.

link-state-id: Link state ID, an IPv4 address.

originate-router *router-id*: ID of the advertising router .

total: Displays the LSA statistics information in the LSDB.

Description

Use the **display ospfv3 lsdb** command to display OSPFv3 LSDB information.

Examples

Display OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
               Link-LSA (Interface Vlan-interface100)
 ------------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix
2.50.0.99       1.1.1.1          0212  0x80000002 0x1053      1

               Router-LSA (Area 0.0.0.0)
 ------------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum    Link
0.0.0.0         1.1.1.1          0167  0x80000004 0x0a21      0

               Intra-Area-Prefix-LSA (Area 0.0.0.0)
 ------------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix  Reference
0.0.0.1         1.1.1.1          0162  0x80000004 0x0cac      1  Router-LSA
```

Table 1-3 display ospfv3 lsdb command output description

Field	Description
Link-LSA	Each Link-LSA describes the IPv6 address prefix of the link and Link-local address of the router
Link State ID	Link State ID
Origin Router	Originating Router
Age	Age of LSAs

Field	Description
SeqNum	LSA sequence number
CkSum	LSA Checksum
Prefix	Number of Prefixes
Router-LSA	Originated by all routers. This LSA describes the collected states of the router's interfaces to an area. Flooded throughout a single area only.
Link	Number of links
Intra-Area-Prefix-LSA	Each Intra-Area-Prefix-LSA contains IPv6 prefix information on a router, stub area or transit area information
Reference	Type of referenced LSA

Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link

           OSPFv3 Router with ID (1.1.1.1) (Process 1)

               Link-LSA (Interface Vlan-interface100)
 ------------------------------------------------------------------
  LS age            : 634
  LS Type           : Link-LSA
  Link State ID     : 2.50.0.99
  Originating Router: 1.1.1.1
  LS Seq Number     : 0x80000002
  Checksum          : 0x1053
  Length            : 56
  Priority          : 1
  Options           : 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: FE80::200:FCFF:FE00:6505
  Number of Prefixes: 1
      Prefix        : 1::/64
      Prefix Options: 0 (-|-|-|-)
```

Table 1-4 display ospfv3 lsdb command output description

Field	Description
LS age	Age of LSA
LS Type	Type of LSA
Originating Router	Originating Router
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Priority	Router Priority
Options	Options
Link-Local Address	Link-Local Address

Field	Description
Number of Prefixes	Number of Prefixes
Prefix	Address prefix
Prefix Options	Prefix options

display ospfv3 lsdb statistic

Syntax

display ospfv3 lsdb statistic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ospfv3 lsdb statistic** command to display LSA statistics in the OSPFv3 LSDB.

Examples

Display OSPFv3 LSDB statistics.

```
<System> display ospfv3 lsdb statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                        LSA Statistics
 ----------------------------------------------------------------------
Area ID         Router   Network  InterPre InterRou IntraPre Link     ASE
0.0.0.0         2        1        1        0        1
0.0.0.1         1        0        1        0        1
Total           3        1        2        0        2        3        0
```

Table 1-5 Descriptions on the fields of the **display ospfv3 lsdb statistic** command output description

Field	Description
Area ID	Area ID
Router	Router-LSA number
Network	Network-LSA number
InterPre	Inter-Area-Prefix-LSA number
InterRou	Inter-Area-Router-LSA number
IntraPre	Intra-Area-Prefix-LSA number
Link	Link-LSA number

Field	Description
ASE	AS-external-LSA number
Total	Total LSA number

display ospfv3 next-hop

Syntax

display ospfv3 [*process-id*] **next-hop**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

Description

Use the **display ospfv3 next-hop** command to display OSPFv3 next hop information.

If no process is specified, next hop information of all OSPFv3 processes is displayed.

Examples

Display OSPFv3 next hop information.

```
<Sysname> display ospfv3 next-hop

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id     Next-Hop                                Interface   RefCount
1.1.1.1         FE80::20F:E2FF:FE00:1                   Vlan100      1
```

Table 1-6 display ospfv3 next-hop command output description

Field	Description
Neighbor-Id	Neighboring router ID
Next-hop	Next-hop address
Interface	Outbound interface
RefCount	Reference count

display ospfv3 peer

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

area: Specifies to display neighbor information of the specified area.

area-id: The ID of an area, a decimal integer that is translated into IPv4 address format by the system (in the range of 0 to 4294967295) or an IPv4 address.

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

verbose: Display detailed neighbor information.

peer-router-id: Router-ID of the specified neighbor.

Description

Use the **display ospfv3 peer** command to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

Examples

Display the neighbor information of OSPFv3 process 1 on an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 10
                    OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1         1     Full/ -         00:00:30    vlan10     0
```

Table 1-7 display ospfv3 peer command output description

Field	Description
Neighbor ID	Router ID of a neighbor
Pri	Priority of neighbor router
State	Neighbor state
Dead Time	Dead time remained
Interface	Interface connected to the neighbor
Instance ID	Instance ID

Display detailed neighbor information of OSPFv3 process 100 of an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 33 verbose

                    OSPFv3 Process (1)
 Neighbor 1.1.1.1 is Full, interface address FE80::200:FCFF:FE00:6505
```

```
In the area 0.0.0.0 via interface Vlan-interface100
DR is 1.1.1.1 BDR is 1.1.1.2
Options is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:33
Neighbor is up for 00:00:17
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
```

Table 1-8 display ospfv3 peer verbose command output description

Field	Description
Neighbor	Neighbor ID
interface address	Interface address
In the area 0.0.0.0 via interface Vlan-interface100	Interface Vlan-interface100 belongs to area 0
DR is 1.1.1.1 BDR is 1.1.1.2	DR is 1.1.1.1 BDR is 1.1.1.2
Options is 0x000013 (-|R|-|-|E|V6)	The option is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:33	Dead timer due in 00:00:33
Neighbor is up for 00:00:17	Neighbor is up for 00:00:17
Database Summary List	Number of LSAs sent in DD packet
Link State Request List	Number of LSAs in the link state request list
Link State Retransmission List	Number of LSAs in the link state retransmission list

display ospfv3 peer statistic

Syntax

display ospfv3 peer statistic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ospfv3 peer statistic** command to display information about all OSPFv3 neighbors on the router, that is, numbers of neighbors in different states.

Examples

Display information about all OSPFv3 neighbors.

```
<Sysname> display ospfv3 peer statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          Neighbor Statistics
 ------------------------------------------------------------------------
Area ID         Down     Init     2-way    ExStar   Exchange Loading  Full
0.0.0.0         0        0        0        0        0        0        1
Total           0        0        0        0        0        0        1
```

Table 1-9 display ospfv3 peer statistic command output description

Field	Description
Area ID	Area ID
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no Router ID of the neighbor. Mutual communication is not setup.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and master/slave relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

display ospfv3 request-list

Syntax

display ospfv3 [*process-id*] **request-list** [{ **external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router** } [*link-state-id*] [**originate-router** *ip-address*] | **statistics**]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPFv3 process ID, in the range 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state request list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state request list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state request list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state request list.

link: Displays the Link LSA information of the OSPFv3 link state request list.

network: Displays the Network-LSA information of the OSPFv3 link state request list.

router: Displays the Router-LSA information of the OSPFv3 link state request list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router *ip-address*: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state request list.

Description

Use the **display ospfv3 request-list** command to display OSPFv3 link state request list information.

If no process is specified, the link state request list information of all OSPFv3 processes is displayed.

Examples

Display the information of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list
         OSPFv3 Router with ID (11.1.1.1) (Process 1)
             Interface Vlan100    Area-ID 0.0.0.0
----------------------------------------------------------------------------
                          Nbr-ID   12.1.1.1
LS-Type               LS-ID           AdvRouter       SeqNum       Age  CkSum
Router-LSA            0.0.0.0         12.1.1.1          0x80000014    774  0xe5b0
```

Table 1-10 display ospfv3 request-list command output description

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising router
SeqNum	LSA sequence number
Age	Age of LSA
CkSum	Checksum

Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics
            OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface  Neighbor        LSA-Count
Vlan100     10.1.1.1        0
```

Table 1-11 display ospfv3 request-list statistics command output description

Field	Description
Interface	Interface name
Neighbor	Neighbor router ID

Field	Description
LSA-Count	Number of LSAs in the request list

display ospfv3 retrans-list

Syntax

display ospfv3 [*process-id*] **retrans-list** [{ **external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router** } [*link-state-id*] [**originate-router** *ip-address*] | **statistics**]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPFv3 process ID, in the range 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state retransmission list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state retransmission list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state retransmission list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state retransmission list.

link: Displays the Link LSA information of the OSPFv3 link state retransmission list.

network: Displays the Network-LSA information of the OSPFv3 link state retransmission list.

router: Displays the Router-LSA information of the OSPFv3 link state retransmission list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router *ip-address*: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state retransmission list.

Description

Use the **display ospfv3 retrans-list** command to display the OSPFv3 link state retransmission list.

If no process is specified, the link state retransmission list information of all OSPFv3 processes is displayed.

Examples

Display the information of the OSPFv3 link state retransmission list.

```
<Sysname> display ospfv3 retrans-list
            OSPFv3 Router with ID (11.1.1.1) (Process 1)
             Interface Vlan100    Area-ID 0.0.0.0
----------------------------------------------------------------------------
Nbr-ID   12.1.1.1
LS-Type              LS-ID           AdvRouter       SeqNum       Age  CkSum
Link-LSA             0.15.0.24       12.1.1.1          0x80000003    519  0x7823
```

```
Router-LSA          0.0.0.0         12.1.1.1         0x80000014    774  0xe5b0
```

Table 1-12 display ospfv3 retrans-list command output description

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising Router
SeqNum	LSA sequence Number
Age	Age of LSA
CkSum	Checksum

Display the statistics of OSPFv3 link state retransmission list.

```
<Sysname>display ospfv3 retrans-list statistics
            OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface  Neighbor        LSA-Count
Vlan100     12.1.1.1        2
```

Table 1-13 display ospfv3 retrans-list statistics command output description

Field	Description
Interface	Interface name
Neighbor	Neighbor ID
LSA-Count	Number of LSAs in the retransmission request list

display ospfv3 routing

Syntax

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length* **|** *ipv6-address/prefix-length* | **abr-routes** | **asbr-routes** | **all | statistics**]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length, in the range 0 to 128.

abr-routes: Displays routes to ABR.

asbr-routes: Displays routes to ASBR.

all: Displays all routes.

statistics: Displays the OSPFv3 routing table statistics .

Description

Use the **display ospfv3 routing** command to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

Examples

Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing

 E1 - Type 1 external route,    IA - Inter area route,    I  - Intra area route
 E2 - Type 2 external route,    *  - Seleted route

           OSPFv3 Router with ID (1.1.1.1) (Process 1)
 ------------------------------------------------------------------------
 *Destination: 2001::/64
  Type       : I                                    Cost     : 1
  NextHop    : directly-connected                   Interface: Vlan100
```

Table 1-14 display ospfv3 routing command output description

Field	Description
Destination	Destination network segment
Type	Route type
Cost	Route cost value
Next-hop	Next hop address
Interface	Outbound interface

Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
           OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          OSPFv3 Routing Statistics
 Intra-area-routes   :   1
 Inter-area-routes   :   0
 External-routes     :   0
```

Table 1-15 display ospfv3 routing statistics command output description

Field	Description
Intra-area-routes	Number of Intra-area-routes
Inter-area-routes	Number of inter-area routes

Field	Description
External-routes	Number of external routes

display ospfv3 statistics

Syntax

display ospfv3 statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ospfv3 statistics** command to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

Examples

Display outbound/inbound OSPFv3 packet statistics on associated interfaces.

```
<Sysname> display ospfv3 statistics

                     OSPFv3 Statistics
Interface Vlan-interface100 Instance 0
 Type              Input       Output
 Hello             189         63
 DB Description    10          8
 Ls Req            2           1
 Ls Upd            16          6
 Ls Ack            10          6
 Discarded          0           0
```

Table 1-16 display ospfv3 statistics command output description

Field	Description
Interface	Interface name
Instance	Instance number
Type	Type of packet
Input	Number of packets received by the interface
Output	Number of packets sent by the interface
Hello	Hello packet

Field	Description
DB Description	Database description packet
Ls Req	Link state request packet
Ls Upd	Link state update packet
Ls Ack	Link state acknowledgement packet
Discarded	Discarded packet

display ospfv3 topology

Syntax

display ospfv3 [*process-id*] **topology** [**area** *area-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Displays the topology information of an OSPFv3 process; The process ID ranges from 1 to 65535.

area: Displays the topology information of the specified area.

area-id: ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

Description

Use the **display ospfv3 topology** command to display OSPFv3 topology information. If no process is specified, topology information of all OSPFv3 processes is displayed.

Examples

Display OSPFv3 area 1 topology information.

```
<Sysname> display ospfv3 topology area 1
                    OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)       Bits      Metric    Next-Hop        Interface
Rtr   1.1.1.1                     --
Rtr   2.2.2.2                     1         2.2.2.2         Vlan100
```

Table 1-17 display ospfv3 topology command output description

Field	Description
Type	Type of node
ID(If-Index)	Router ID
Bits	Flag bit

Field	Description
Metric	Cost value
Next-Hop	Next hop
Interface	Outbound interface

display ospfv3 vlink

Syntax

display ospfv3 [*process-id*] **vlink**

View

Any view

Default Level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

Description

Use the **display ospfv3 vlink** command to display OSPFv3 virtual link information. If no process is specified, virtual link information of all OSPFv3 processes is displayed.

Examples

Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink
     Virtual Link VLINK1 to router 1.1.1.1 is up
       Transit area :0.0.0.1 via interface Vlan-interface100, instance ID: 0
       Local address: 2000:1::1
       Remote address: 2001:1:1::1
       Transmit Delay is 1 sec, State: P-To-P,
       Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
         Hello due in 00:00:02
         Adjacency state :Full
```

Table 1-18 display ospfv3 vlink command output description

Field	Description
Virtual Link VLINK1 to router 1.1.1.1 is up	The virtual link VLINK1 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface Vlan-interface100	Interface Vlan-interface100 in transit area 0.0.0.1.
instance ID	Instance ID
Local address	Local IPv6 address
Remote address	Remote IPv6 address

Field	Description
Transmit Delay	Transmit delay of sending LSAs
State	Interface state
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Timer intervals in seconds, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Send hello packets in 2 seconds.
Adjacency state	Adjacency state

filter-policy export (OSPFv3 view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

undo filter-policy export [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

View

OSPFv3 view

Default Level

2: System level

Parameters

acl6-number: Specifies the ACL6 number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

isisv6 *process-id*: Specifies to filter the routes of an IPv6-IS-IS process, which is in the range of 1 to 65535.

ospfv3 *process-id*: Specifies to filter the routes of an OSPFv3 process, which is in the range of 1 to 65535.

ripng *process-id*: Specifies to filter the routes of a RIPng process, which in the range of 1 to 65535.

bgp4+: Specifies to filter BGP4+ routes.

direct: Specifies to filter direct routes.

static: Specifies to filter static routes.

Description

Use the **filter-policy export** command to filter redistributed routes.

Use the **undo filter-policy export** command to remove the configuration.

If no protocol is specified, all redistributed routes will be filtered.

By default, IPv6 OSPFv3 does not filter redistributed routes.

Note

Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, use of the **filter-policy export** command does not take effect.

Examples

Filter all redistributed routes using IPv6 ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2001] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

filter-policy import (OSPFv3 view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View

OSPFv3 view

Default Level

2: System level

Parameters

acl6-number: Specifies an ACL number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

Description

Use the **filter-policy import** command to configure OSPFv3 to filter routes computed from received LSAs.

Use the **undo filter-policy import** command to remove the configuration.

By default, OSPFv3 does not filter routes computed from received LSAs.

Note

Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.

Examples

Filter received routes using the IPv6 prefix list abc.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import
```

import-route (OSPFv3 view)

Syntax

import-route { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** [**allow-ibgp**] | **direct** | **static** } [**cost** *value* | **type** *type* | **route-policy** *route-policy-name*] *

undo import-route { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static** }

import-route *protocol* [*process-id* | **allow-ibgp**] [**cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View

OSPFv3 view

Default Level

2: System level

Parameters

protocol: Redistributes routes from a specified routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospf v3**, **ripng**, or **static**.

process-id: Process ID of the routing protocol, in the range 1 to 65536. It defaults to 1. This argument takes effect only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

allow-ibgp: Allows redistributing iBGP routes. This keyword takes effect only the protocol is **bgp4+**.

cost *cost*: Specifies a cost for redistributed routes, ranging from 1 to 16777214. The default is 1.

type *type*: Specifies the type for redistributed routes, 1 or 2. It defaults to 2.

route-policy *route-policy-name*: Specifies to redistribute only the routes that match the specified route policy. *route-policy-name* is a string of 1 to 19 characters.

 **Caution**

Using the **import-route bgp4+** command redistributes only EBGP routes, while using the **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes.

Description

Use the **import-route** command to redistribute routes.

Use the **undo import-route** command to disable routes redistribution.

IPv6 OSPFv3 does not redistribute routes from other protocols by default.

Examples

Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes found by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

OSPFv3 view

Default Level

2: System level

Parameters

None

Description

Use the **log-peer-change** command to enable the logging on neighbor state changes.

Use the **undo maximum load-balancing** command to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

Examples

Disable the logging on neighbor state changes of OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

maximum load-balancing (OSPFv3 view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPFv3 view

Default Level

2: System level

Parameters

maximum: Maximum number of equal-cost routes for load-balancing. Its value is in the range 1 to 4. The argument being set to 1 means no load balancing is available.

Description

Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load-balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost routes for load-balancing in OSPFv3 is 4.

Examples

Configure the maximum number of equal-cost routes for load-balancing as 2.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 2
```

ospfv3

Syntax

ospfv3 [*process-id*]

undo ospfv3 [*process-id*]

View

System view

Default Level

2: System level

Parameters

process-id: OSPFv3 process ID, ranging from 1 to 65535. The process ID defaults to 1.

Description

Use the **ospfv3** command to enable an OSPFv3 process and enter OSPFv3 view.

Use the **undo ospfv3** command to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

Related commands: **router-id**.

Note

An OSPFv3 process can run normally only when Router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.

Examples

Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

process-id: OSPFv3 process ID, in the range 1 to 65535.

area-id: Area ID, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

instance-id: Instance ID of an interface, in the range 0 to 255. The default is 0.

Description

Use the **ospfv3 area** command to enable an OSPFv3 process on the interface and specify the area for the interface.

Use the **undo ospfv3 area** command to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

Examples

Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

ospfv3 cost

Syntax

ospfv3 cost *value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

value: OSPFv3 cost of the interface, in the range 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use the **ospfv3 cost** command to configure the OSPFv3 cost of the interface in an instance.

Use the **undo ospfv3 cost** command to restore the default OSPFv3 cost of the interface in an instance.

By default, a router's interface automatically calculates the OSPFv3 cost based on its bandwidth. For a VLAN interface of a switch, the cost value defaults to 1.

Examples

Specifies the OSPFv3 cost of the interface in instance 1 as 33 .

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Syntax

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

priority: DR priority, in the range 0 to 255.

instance-id: ID of the instance an interface belongs to, in the range 0 to 255, which defaults to 0.

Description

Use the **ospfv3 dr-priority** command to set the DR priority for an interface in an instance.

Use the **undo ospfv3 dr-priority** command to restore the default value.

The DR priority on an interface defaults to 1.

An interface's DR priority determines its privilege in DR/BDR selection, and the interface with the highest priority is preferred.

Examples

Set the DR priority for an interface in instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

ospfv3 mtu-ignore

Syntax

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

instance-id: Instance ID, in the range 0 to 255, which defaults to 0.

Description

Use the **ospfv3 mtu-ignore** command to configure an interface to ignore MTU check during DD packet exchange.

Use the **undo ospfv3 mtu-ignore** command to restore the default.

By default, an interface performs MTU check during DD packet exchange. A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Examples

Configure an interface that belongs to instance 1 to ignore MTU check during DD packet exchange.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

ospfv3 network-type

Syntax

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

broadcast: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

non-broadcast: Specifies the interface to send packets in unicast mode. By default, an OSPFv3 interface whose network type is P2MP sends packets in multicast mode.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use the **ospfv3 network-type** command to set the network type for an OSPFv3 interface.

Use the **undo ospfv3 network-type** command to restore the default.

By default, the network type of an interface depends on its link layer protocol. For example:

- For PPP, the default network type is P2P.
- For Ethernet, the default network type is broadcast.

Examples

Configure the interface's network type as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 network-type nbma
```

ospfv3 peer

Syntax

ospfv3 peer *ipv6-address* [**dr-priority** *dr-priority*] [**instance** *instance-id*]

undo ospfv3 peer *ipv6-address* [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

ipv6-address: Neighbor link-local IP address.

dr-priority: Neighbor DR priority, in the range 0 to 255. The default is 1.

instance-id: Interface instance ID, in the range 0 to 255. The default is 0.

Description

Use the **ospfv3 peer** command to specify a neighbor and the DR priority of the neighbor.

Use the **undo ospfv3 peer** command to remove the configuration.

A router uses the priority set with the **ospfv3 peer** command to determine whether to send a hello packet to the neighbor rather than for DR election.

Examples

Specify the neighbor fe80::1111.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 peer fe80::1111
```

ospfv3 timer dead

Syntax

ospfv3 timer dead *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

seconds: Dead time in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use the **ospfv3 timer dead** command to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use the **undo ospfv3 timer dead** command to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds for P2P and Broadcast interfaces, and is not supported on P2MP and NBMA interfaces at present.

OSPFv3 neighbor dead time: if an interface receives no hello packet from a neighbor after dead time elapses, the interface will consider the neighbor dead.

The **dead** *seconds* value is at least four times the **Hello** *seconds* value and must be identical on interfaces attached to the same network segment.

Note

Currently, the S7900E series Ethernet switches do not support configuring the **ospfv3 timer dead** command on a loopback interface.

Related commands: **ospfv3 timer hello**.

Examples

Configure the OSPFv3 neighbor dead time as 80 seconds for the interface in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 80 instance 1
```

ospfv3 timer hello

Syntax

ospfv3 timer hello *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

seconds: Interval between hello packets, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use the **ospfv3 timer hello** command to configure the hello interval for an interface that belongs to an instance.

Use the **undo ospfv3 timer hello** command to restore the default .

By default, the hello interval is 10 seconds for P2P and Broadcast interfaces, and is not supported on the P2MP or NBMA interfaces at present.

Note

Currently, the S7900E series Ethernet switches do not support configuring the **ospfv3 timer hello** command on a loopback interface.

Related commands: **ospfv3 timer dead**.

Examples

Configure the hello interval as 20 seconds for an interface in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer hello 20 instance 1
```

ospfv3 timer retransmit

Syntax

ospfv3 timer retransmit *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

interval: LSA retransmission interval in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use the **ospfv3 timer retransmit** command to configure the LSA retransmission interval for an interface in an instance.

Use the **undo ospfv3 timer retransmit** command to restore the default.

The interval defaults to 5 seconds.

After sending a LSA to its neighbor, the device waits for an acknowledgement. If receiving no acknowledgement after the LSA retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

Note

Currently, the S7900E series Ethernet switches do not support configuring the **ospfv3 timer retransmit** command on a loopback interface.

Examples

Configure the LSA retransmission interval on an interface in instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

ospfv3 timer poll

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

seconds: Poll interval in seconds, in the range 1 to 65535.

instance-id: Interface instance ID, in the range 0 to 255. The default is 0.

Description

Use the **ospfv3 timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospfv3 timer poll** command to restore the default value.

By default, the poll interval is 120 seconds.

Note

Currently, the S7900E series Ethernet switches do not support configuring the **ospfv3 timer poll** command on a loopback interface.

Examples

Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

ospfv3 trans-delay

Syntax

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

View

Interface view

Default Level

2: System level

Parameters

seconds: Transmission delay in seconds, ranging from 1 to 3600.

instance-id: Instance ID of an interface, in the range of 0 to 255, with the default as 0.

Description

Use the **ospfv3 trans-delay** command to configure the transmission delay for an interface with an instance ID.

Use the **undo ospfv3 trans-delay** command to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented by 1 every second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

Note

Currently, the S7900E series Ethernet switches do not support configuring the **ospfv3 trans-delay** command on a loopback interface.

Examples

Configure the transmission delay as 3 seconds for an interface in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

preference

Syntax

preference [**ase**] [**route-policy** *route-policy-name*] *preference*

undo preference [**ase**]

View

OSPFv3 view

Default Level

2: System level

Parameters

ase: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

route-policy *route-policy-name*: References a routing policy to set preference for specific routes. The name is a string of 1 to 19 characters.

Preference: Preference of OSPFv3, in the range 1 to 255.

Description

Use the **preference** command to specify a preference for OSPFv3 routes.

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

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A router may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples

Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

router-id

Syntax

router-id *router-id*

undo router-id

View

OSPFv3 view

Default Level

2: System level

Parameters

router-id: 32-bit router ID, in IPv4 address format.

Description

Use the **router-id** command to configure the OSPFv3 router ID.

Use the **undo router-id** command to remove a configured router ID.

Router ID is the unique identifier of a device running an OSPFv3 process in the autonomous system. The OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

Related commands: **ospfv3**.

Note

By configuring different router IDs for different processes, you can run multiple OSPFv3 processes on a router.

Examples

Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

silent-interface(OSPFv3 view)

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

View

OSPFv3 view

Default Level

2: System level

Parameters

interface-type interface-number: Interface type and number

all: Specifies all interfaces.

Description

Use the **silent-interface** command to disable the specified interface from sending OSPFv3 packets.

Use the **undo silent-interface** command to restore the default.

An interface is able to send OSPFv3 packets by default.

Multiple processes can disable the same interface from sending OSPFv3 packets, but use of the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples

Disable an interface from sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.110.1.9
[Sysname-ospfv3-100] silent-interface vlan-interface 10
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.18.0.7
[Sysname-ospfv3-200] silent-interface vlan-interface 10
```

spf timers

Syntax

spf timers *delay-interval hold-interval*

undo spf timers

View

OSPFv3 view

Default Level

2: System level

Parameters

delay-interval: Interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation. in the range 1 to 65535.

hold-interval: Hold interval in seconds between two consecutive SPF calculations, in the range 1 to 65535.

Description

Use the **spf timers** command to configure the delay interval and hold interval for OSPFv3 SPF calculation.

Use the **undo spf timers** command to restore the default.

The delay interval and hold interval default to 5s and 10s.

An OSPFv3 router works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree. Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.

Examples

Configure the delay interval and hold interval as 6 seconds for SPF calculation.

```
<Sysname> system-view
[Sysname]ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

stub (OSPFv3 area view)

Syntax

stub [**no-summary**]

undo stub

View

OSPFv3 area view

Default Level

2: System level

Parameters

no-summary: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).

Description

Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

By default, an area is not configured as a stub area.

When an area is configured as a stub area, all the routers attached to the area must be configured with the **stub** command.

Related commands: **default-cost**.

Examples

Configure OSPFv3 area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

vlink-peer (OSPFv3 area view)

Syntax

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **instance** *instance-id*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead**] *

View

OSPFv3 area view

Default Level

2: System level

Parameters

router-id: Router ID for a virtual link neighbor.

hello *seconds*: Specifies the interval in seconds for sending Hello packets, ranging from 1 to 8192, with the default as 10. This value must be equal to the **hello** *seconds* configured on the virtual link peer.

retransmit *seconds*: Specifies the interval in seconds for retransmitting LSA packets, ranging from 1 to 3600, with the default as 5.

trans-delay *seconds*: Specifies the delay interval in seconds for sending LSA packets, ranging from 1 to 3600, with the default as 1.

dead *seconds*: Specifies the neighbor dead time in seconds, ranging from 1 to 32768, with the default as 40. This value must be equal to the **dead** *seconds* configured on the virtual link peer, and at least four times the value of **hello** *seconds*.

instance *Instance-id*: Instance ID of an virtual link, in the range of 0 to 255, with the default as 0.

Description

Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

For a non-backbone area without a direct connection to the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical links. A virtual link

can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **dead**, **retransmit** and **trans-delay** are configured in the similar way.

Both ends of a virtual link are ABRs that are configured with the **vlink-peer** command.

Examples

Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 10.0.0.0
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

Table of Contents

1 IPv6 IS-IS Configuration Commands

IPv6 IS-IS Configuration Commands

Note

- The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.
- IPv6 IS-IS supports all the features of IPv4 IS-IS except that it advertises IPv6 routing information instead. This document describes only IPv6 IS-IS exclusive commands. Refer to *IS-IS Commands* in the *IP Routing Volume* for other IS-IS configuration commands.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

display isis route ipv6

Syntax

display isis route ipv6 [[**level-1** | **level-2**] | **verbose**] * [*process-id*]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed IPv6 IS-IS routing information.

process-id: IS-IS process ID, in the range 1 to 65535.

level-1: Display Level-1 IPv6 IS-IS routes only.

level-2: Displays Level-2 IPv6 IS-IS routes only.

Note

If no level is specified, both Level-1 and Level-2 (namely Level-1-2) routing information will be displayed.

Description

Use the **display isis route ipv6** command to display IPv6 IS-IS routing information.

Examples

Display IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6

                        Route information for ISIS(1)
                        ----------------------------

                    ISIS(1) IPv6 Level-1 Forwarding Table
                    -------------------------------------
 Destination: 2001:2::                              PrefixLen: 64
 Flag       : D/L/-                                   Cost     : 10
 Next Hop   : Direct                                 Interface: Vlan200

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 1-1 display isis route ipv6 command output description

Field	Description
Destination	IPv6 destination address prefix
PrefixLen	Length of the prefix
Flag/Flags	Flag of routing information status D: This is a direct route. R: The route has been added into the routing table. L: The route has been advertised in a LSP. U: Route leaking flag, indicating the Level-1 route is from Level-2. **U** means the route will not be returned to Level-2.
Cost	Value of cost
Next Hop	Next hop
Interface	Outbound interface

Display detailed IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6 verbose
                        Route information for ISIS(1)
                        ----------------------------

                    ISIS(1) IPv6 Level-1 Forwarding Table
                    -------------------------------------
 IPV6 Dest   : 2001:1::/64                 Cost : 20           Flag : R/-/-
 Admin Tag   : -                        Src Count : 2
 NextHop     :                          Interface :          ExitIndex :
    FE80::200:FCFF:FE00:7507                Vlan200              0x00000003

 IPV6 Dest   : 2001:2::/64                  Cost : 10           Flag : D/L/-
 Admin Tag   : -                        Src Count : 2
 NextHop     :                          Interface :          ExitIndex :
```

```
Direct                                    Vlan200              0x00000000

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 1-2 display isis route ipv6 verbose command output description

Field	Description
IPV6 Dest	IPv6 destination
Cost	Value of cost
Flag/Flags	Flag of routing information status D: This is a direct route. R: The route has been added into the routing table. L: The route has been advertised in a LSP. U: Route leaking flag, indicating the Level-1 route is from Level-2. **U** means the route will not be returned to Level-2.
Admin Tag	Administrative tag
Src Count	Number of advertisement sources
Next Hop	Next hop
Interface	Outbound interface
ExitIndex	Outbound interface index

ipv6 default-route-advertise

Syntax

ipv6 default-route-advertise [[**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name*] *

undo ipv6 default-route-advertise [**route-policy** *route-policy-name*]

View

IS-IS view

Default Level

2: System level

Parameters

route-policy-name: Specifies the name of a routing policy with a string of 1 to 19 characters.

level-1: Specifies the default route as Level-1.

level-2: Specifies the default route as Level-2.

level-1-2: Specifies the default route as Level-1-2.

Note

If no level is specified, the default route belongs to Level-2.

Description

Use the **ipv6 default-route-advertise** command to generate a Level-1 or Level-2 IPv6 IS-IS default route.

Use the **undo ipv6 default-route-advertise** command to disable generating a default route.

No IPv6 IS-IS default route is generated by default.

With a routing policy, you can configure IPv6 IS-IS to generate the default route that must match the routing policy. You can use the **apply isis level-1** command in routing policy view to generate a default route in L1 LSPs, or use the **apply isis level-2** command in routing policy view to generate a default route in L2 LSPs, and use the **apply isis level-1-2** in routing policy view to generate a default route in L1 and L2 LSPs respectively.

Refer to *Routing Policy Commands* in the *IP Routing Volume* for information about the **apply isis** command.

Examples

Configure the router to generate a default route in Level-2 LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 default-route-advertise
```

ipv6 enable

Syntax

ipv6 enable

undo ipv6 enable

View

IS-IS view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 enable** command to enable IPv6 for the IPv6 IS-IS process.

Use the **undo ipv6 enable** command to disable IPv6.

IPv6 is disabled by default.

Examples

Create IS-IS routing process 1, and enable IPv6 for the process.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
```

ipv6 filter-policy export

Syntax

ipv6 filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo ipv6 filter-policy export [*protocol* [*process-id*]]

View

IS-IS view

Default Level

2: System level

Parameters

acl6-number: Number of a basic or advanced IPv6 ACL used to filter redistributed routes before advertisement, ranging from 2000 to 3999. Refer to *ACL Configuration* in the *Security Volume* for ACL information.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to *Routing Policy Configuration* in the *IP Routing Volume* for IPv6 prefix list information.

route-policy-name: Name of a routing policy used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to *Routing Policy Configuration* in the *IP Routing Volume* for routing policy information.

protocol: Filter routes redistributed from the specified routing protocol before advertisement. The routing protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present. If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.

process-id: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description

Use the **ipv6 filter-policy export** command to configure IPv6 IS-IS to filter redistributed routes before advertisement.

Use the **undo ipv6 filter-policy export** command to disable the filtering.

The filtering is disabled by default.

In some cases, only routes satisfying certain conditions will be advertised. You can configure the filtering conditions using the **ipv6 filter-policy** command.

You can use the **ipv6 filter-policy export** command, which filters redistributed routes only when they are advertised to other routers, in combination with the **ipv6 import-route** command.

- If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.
- If a protocol is specified, only routes redistributed from the protocol are filtered before advertisement.

Related commands: **ipv6 filter-policy import**.

Examples

Reference the ACL6 2006 to filter all the redistributed routes before advertisement.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2006 export
```

ipv6 filter-policy import

Syntax

ipv6 filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo ipv6 filter-policy import

View

IS-IS view

Default Level

2: System level

Parameters

acl6-number: Number of a basic or advanced IPv6 ACL used to filter incoming routes, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter incoming routes, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter incoming routes, a string of 1 to 19 characters.

Description

Use the **ipv6 filter-policy import** command to configure IPv6 IS-IS to filter the received routes.

Use the **undo ipv6 filter-policy import** command to disable the filtering.

The filtering is disabled by default.

In some cases, only the routing information satisfying certain conditions will be received. You can configure the filtering conditions using the **ipv6 filter-policy** command.

Related commands: **ipv6 filter-policy export**.

Examples

Reference the IPv6 ACL 2003 to filter the received routes.

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1] ipv6 filter-policy 2003 import
```

ipv6 import-route

Syntax

ipv6 import-route *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | [**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo ipv6 import-route *protocol* [*process-id*]

View

IS-IS view

Default Level

2: System level

Parameters

protocol: Redistributes routes from a specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+** or **ospfv3**.

process-id: Process ID of the routing protocol of **ripng**, **isisv6** or **ospfv3**, in the range of 1 to 65535. The default is 1.

cost: Cost for redistributed routes, ranging from 0 to 4261412864.

level-1: Redistributes routes into Level-1 routing table.

level-2: Redistributes routes into Level-2 routing table.

level-1-2: Redistributes routes into Level-1 and Level-2 routing tables.

route-policy-name: Name of a routing policy used to filter routes when they are being redistributed, a string of 1 to 19 characters.

tag: Specifies a administrative tag number for the redistributed routes, in the range of 1 to 4294967295.

allow-ibgp: Allows to redistribute IBGP routes. This keyword is optional when the *protocol* is **bgp4+**.

Description

Use the **ipv6 import-route** command to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use the **undo ipv6 import-route** command to disable route redistribution.

Route redistribution is disabled by default.

If no level is specified, the routes are imported to Level-2 routing table by default.

IPv6 IS-IS considers redistributed routes as routes to destinations outside the local routing domain.

You can specify a cost and a level for redistributed routes.

Caution

Using the **import-route bgp4+ allow-ibgp** command will redistribute both EBGP and IBGP routes. The redistributed IBGP routes may cause routing loops. Therefore, be cautious with this command.

Examples

Configure IPv6–IS-IS to redistribute static routes and set the cost 15 for them.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]ipv6 import-route static cost 15
```

ipv6 import-route isisv6 level-2 into level-1

Syntax

ipv6 import-route isisv6 level-2 into level-1 [**filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo ipv6 import-route isisv6 level-2 into level-1

View

IS-IS view

Default Level

2: System level

Parameters

acl6-number: Number of a basic or advanced ACL6 used to filter routes when they are leaking from Level-2 to Level-1, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

tag: Specifies a administrative tag number for the leaked routes, in the range of 1 to 4294967295.

Description

Use the **ipv6 import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route leaking from Level-2 to Level-1.

Use the **undo ipv6 import-route isisv6 level-2 into level-1** command to disable the leaking.

The leaking is disabled by default.

The route leaking feature enables a Level-1-2 router to advertise routes destined to the Level-2 area and other Level-1 areas to the Level-1 and Level-1-2 routers in the local area.

Examples

Enable IPv6 IS-IS route leaking from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route isisv6 level-2 into level-1
```

ipv6 import-route limit

Syntax

ipv6 import-route limit *number*

undo ipv6 import-route limit

View

IS-IS view

Default Level

2: System level

Parameters

number: Maximum number of redistributed Level 1/Level 2 IPv6 routes. The default varies with devices.

Description

Use the **ipv6 import-route limit** command to configure the maximum number of redistributed Level 1/Level 2 IPv6 routes.

Use the **undo ipv6 import-route limit** command to restore the default.

The default varies with devices.

Examples

Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv6 routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1]ipv6 import-route limit 1000
```

ipv6 maximum load-balancing

Syntax

ipv6 maximum load-balancing *number*

undo ipv6 maximum load-balancing

View

IS-IS view

Default Level

2: System level

Parameters

number: Maximum number of equal-cost routes for load balancing. Its value is in the range 1 to 4 and defaults to 4.

Description

Use the **ipv6 maximum load-balancing** command to configure the maximum number of equal-cost routes for load balancing.

Use the **undo ipv6 maximum load-balancing** command to restore the default.

Note

Configure the maximum number of equivalent load-balanced routes according to the memory capacity.

Examples

Configure the maximum number of equivalent load-balanced routing as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] ipv6 maximum load-balancing 2
```

ipv6 preference

Syntax

ipv6 preference { *preference* | **route-policy** *route-policy-name* } *

undo ipv6 preference

View

IS-IS view

Default Level

2: System level

Parameters

preference: Preference for IPv6 IS-IS, ranging from 1 to 255.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description

Use the **ipv6 preference** command to configure the preference for IPv6 IS-IS protocol.

Use the **undo ipv6 preference** command to configure the default preference for IPv6 IS-IS protocol.

The default preference is 15.

When a router runs multiple dynamic routing protocols at the same time, the system will assign a preference to each routing protocol. If several protocols find routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples

Configure the preference of IPv6 IS-IS protocol as 20.

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

```
[Sysname] isis
[Sysname-isis-1] ipv6 preference 20
```

ipv6 summary

Syntax

ipv6 summary *ipv6-prefix prefix-length* [**avoid-feedback** | **generate_null0_route** | [**level-1** | **level-1-2** | **level-2**] | **tag** *tag*] *

undo ipv6 summary *ipv6-prefix prefix-length* [**level-1** | **level-1-2** | **level-2**]

View

IS-IS view

Default Level

2: System level

Parameters

ipv6-prefix: IPv6 prefix of the summary route.

prefix-length: Length of the IPv6 prefix, in the range of 0 to 128.

avoid-feedback: Specifies to avoid learning summary routes via routing calculation.

generate_null0_route: Generates the NULL 0 route to avoid routing loops.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to Level-2 area.

tag: Value of a administrative tag, in the range of 1 to 4294967295.

 **Note**

If no level is specified in the command, the default is **level-2**.

Description

Use the **ipv6 summary** command to configure an IPv6 IS-IS summary route.

Use the **undo ipv6 summary** command to remove the summary route.

Route summarization is disabled by default.

Configuring summary routes can reduce the size of the route table, LSPs and LSDB. Routes to be summarized can be IS-IS routes or redistributed routes. The cost of a summary route is the smallest cost among all summarized routes.

Examples

Configure a summary route of 2002::/32.

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1] ipv6 summary 2002:: 32
```

isis ipv6 enable

Syntax

isis ipv6 enable [*process-id*]

undo isis ipv6 enable

View

Interface view

Default Level

2: System level

Parameters

process-id: IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description

Use the **isis ipv6 enable** command to enable IPv6 for the specified IS-IS process on the interface.

Use the **undo isis ipv6 enable** command to disable the configuration.

IPv6 is disabled on the interface by default.

Examples

Enable global IPv6, create IS-IS routing process 1, enable IPv6 for the process, and enable IPv6 for the process on VLAN-interface100.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
[Sysname-isis-1] quit
[Sysname] interface Vlan-interface 100
[Sysname--Vlan-interface100] ipv6 address 2002::1/64
[Sysname--Vlan-interface100] isis ipv6 enable 1
```

Table of Contents

1 IPv6 BGP Configuration Commands

Note

- The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

IPv6 BGP Configuration Commands

balance (IPv6 address family view)

Syntax

balance *number*

undo balance

View

IPv6 address family view

Default Level

2: System level

Parameters

number: Number of BGP routes participating in load balancing. Its value is in the range 1 to 4. When it is set to 1, load balancing is disabled.

Description

Use the **balance** command to configure the number of routes participating in IPv6 BGP load balancing.

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

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Related commands: **display bgp ipv6 routing-table**.

Examples

Set the number of routes participating in IPv6 BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] balance 2
```

bestroute as-path-neglect (IPv6 address family view)

Syntax

bestroute as-path-neglect

undo bestroute as-path-neglect

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute as-path-neglect** command to configure the IPv6 BGP router to not evaluate the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the IPv6 BGP router to use the AS_PATH during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples

Ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

bestroute compare-med (IPv6 address family view)

Syntax

bestroute compare-med

undo bestroute compare-med

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

 **Caution**

After the **bestroute compare-med** command is executed, the **balance** command does not take effect.

Examples

Compare the MED for paths from an AS for selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute compare-med
```

bestroute med-confederation (IPv6 address family view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers for best route selection.

Use the **undo bestroute med-confederation** command to disable the configuration.

By default, this comparison is not enabled.

With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

Compare the MED for paths from peers within the confederation.

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

```
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

compare-different-as-med (IPv6 address family view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths available for one destination, the path with the smallest MED value is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples

Enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] compare-different-as-med
```

dampening (IPv6 address family view)

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv6 address family view

Default Level

2: System level

Parameters

half-life-reachable: Half-life for reachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Half-life for unreachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Reuse threshold value for suppressed routes, in the range 1 to 20000. Penalty value of a suppressed route decreasing under the value is reused. By default, its value is 750.

suppress: Suppression threshold from 1 to 20000, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

ceiling: Ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

half-life-reachable, half-life-unreachable, reuse, suppress and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description

Use the **dampening** command to enable IPv6 BGP route dampening or/and configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter**, **display bgp ipv6 routing-table flap-info**.

Examples

Enable IPv6 BGP route dampening and configure route dampening parameters.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

default local-preference (IPv6 address family view)

Syntax

default local-preference *value*

undo default local-preference

View

IPv6 address family view

Default Level

2: System level

Parameters

value: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Use this command to affect IPv6 BGP route selection.

Examples

Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default local-preference 180
```

default med (IPv6 address family view)

Syntax

default med *med-value*

undo default med

View

IPv6 address family view

Default Level

2: System level

Parameters

med-value: MED value, in the range 0 to 4294967295.

Description

Use the **default med** command to specify the default MED value.

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

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED value. In the

case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

Examples

Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

default-route imported (IPv6 address family view)

Syntax

default-route imported

undo default-route imported

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **default-route imported** command to enable the redistribution of default route into the IPv6 BGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, the redistribution is not enabled.

Examples

Enable the redistribution of default route from OSPFv3 into IPv6 BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

display bgp ipv6 group

Syntax

display bgp ipv6 group [*ipv6-group-name*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-name: Peer group name, a string of 1 to 47 characters.

Description

Use the **display bgp ipv6 group** command to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples

Display the information of the IPv6 peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa

 BGP peer-group is aaa
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer         V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  20:20::20:1  4   200       170       141      0        2 02:13:35 Established
```

Table 1-1 display bgp ipv6 group command output description

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
hold timer value	Holdtime
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval between advertisements
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer

Field	Description
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine state of peer

display bgp ipv6 network

Syntax

display bgp ipv6 network

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 network** command to display IPv6 routes advertised with the **network** command.

Examples

Display IPv6 routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask            Route-policy        Short-cut

  2002::           64
  2001::           64                                  Short-cut
```

Table 1-2 display bgp ipv6 network command output description

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Prefix	Prefix length
Route-policy	Routing policy
Short-cut	Shortcut route

display bgp ipv6 paths

Syntax

display bgp ipv6 paths [*as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

Description

Use the **display bgp ipv6 paths** command to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

Examples

Display IPv6 BGP path information.

```
<Sysname> display bgp ipv6 paths

    Address       Hash    Refcount  MED         Path/Origin
    0x5917098     1       1          0            i
    0x59171D0     9       2          0            100i
```

Table 1-3 display bgp ipv6 paths command output description

Field	Description
Address	Route destination address in local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that used the path
MED	MED of the path

Field	Description	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 peer

Syntax

display bgp ipv6 peer [*group-name* **log-info** | *ipv4-address* **verbose** | *ipv6-address* { **log-info** | **verbose** } | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: Specifies the IPv6 address of a peer to be displayed.

log-info: Displays log information of the specified peer.

verbose: Displays the detailed information of the peer.

Description

Use the **display bgp ipv6 peer** command to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

Examples

Display all IPv6 peer information.

```
<Sysname> display bgp ipv6 peer

 BGP Local router ID : 20.0.0.1
 local AS number : 100
Total number of peers : 1                 Peers in established state : 1

Peer      V    AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down    State
```

```
20::21    4   200  17       19       0          3  00:09:59   Established
```

Table 1-4 display bgp ipv6 peer command output description

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Messages received
MsgSent	Messages sent
OutQ	Messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state

display bgp ipv6 routing-table

Syntax

display bgp ipv6 routing-table [*ipv6-address prefix-length*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

Description

Use the **display bgp ipv6 routing-table** command to display IPv6 BGP routing table information.

Examples

Display the IPv6 BGP routing table.

```
<Sysname> display bgp ipv6 routing-table

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
*>  Network : 30:30::                                   PrefixLen : 64
    NextHop : 30:30::30:1                               LocPrf    :
    PrefVal : 0                                         Label     : NULL
    MED      :0
    Path/Ogn: i

*>  Network : 40:40::                                   PrefixLen : 64
    NextHop : 40:40::40:1                               LocPrf    :
    PrefVal : 0                                         Label     : NULL
    MED     : 0
    Path/Ogn: i
```

Table 1-5 display bgp ipv6 routing-table command output description

Field	Description	
Local router ID	Local router ID	
Status codes	Status codes: * – valid > – best d – damped h – history i – internal (IGP) s – summary suppressed (suppressed) S – Stale	
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by other means)	
Network	Destination network address	
PrefixLen	Prefix length	
NextHop	Next Hop	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
PrefVal	Preferred value	
Label	Label	
Ogn	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates that a route is interior to the AS. Summary routes and the routes configured using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).

Field	Description	
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 routing-table as-path-acl

Syntax

display bgp ipv6 routing-table as-path-acl *as-path-acl-number*

View

Any view

Default Level

1: Monitor level

Parameters

as-path-acl-number: Number of an AS path ACL permitted by which to display routing information, ranging from 1 to 256.

Description

Use the **display bgp ipv6 routing-table as-path-acl** command to display routes filtered through the specified AS path ACL.

Examples

Display routes filtered through the AS path ACL 20.

```
<Sysname> display bgp ipv6 routing-table as-path-acl 20
 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table community

Syntax

display bgp ipv6 routing-table community [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View

Any view

Default Level

1: Monitor level

Parameters

aa:nn: Community number; both aa and nn are in the range 0 to 65535.

&<1-13>: Indicates the argument before it can be entered up to 13 times.

no-advertise: Displays IPv6 BGP routes that cannot be advertised to any peer.

no-export: Displays IPv6 BGP routes that cannot be advertised out the AS; if there is a confederation, it displays IPv6 BGP routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays IPv6 BGP routes that cannot be advertised out the AS or to other sub ASs if a confederation is configured.

whole-match: Displays the IPv6 BGP routes exactly matching the specified community attribute.

Description

Use the **display bgp ipv6 routing-table community** command to display the routing information with the specified community attribute.

Examples

Display the routing information with community attribute no-export.

```
<Sysname> display bgp ipv6 routing-table community no-export
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table community-list

Syntax

display bgp ipv6 routing-table community-list { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View

Any view

Default Level

1: Monitor level

Parameters

basic-community-list-number: Specifies a basic community-list number, in the range 1 to 99.

adv-community-list-number: Specifies an advanced community-list number, in the range 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list-number*.

&<1-16>: Specifies to allow entering the argument before it up to 16 times.

Description

Use the **display bgp ipv6 routing-table community-list** command to view the routing information matching the specified IPv6 BGP community list.

Examples

Display the routing information matching the specified IPv6 BGP community list.

```
<Sysname> display bgp ipv6 routing-table community-list 99
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     :0
     Path/Ogn: i
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table dampened

Syntax

display bgp ipv6 routing-table dampened

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 routing-table dampened** command to display the IPv6 BGP dampened routes.

Examples

Display IPv6 BGP dampened routes.

```
<Sysname> display bgp ipv6 routing-table dampened

BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network : 111::                                  PrefixLen : 64
     From    : 122::1                                 Reuse     : 00:29:34
     Path/Ogn: 200?
```

Table 1-6 display bgp ipv6 routing-table dampened command output description

Field	Description
From	Source IP address of a route
Reuse	Time for reuse

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table dampening parameter

Syntax

display bgp ipv6 routing-table dampening parameter

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 routing-table dampening parameter** command to display IPv6 BGP routing dampening parameters.

Related commands: **dampening**.

Examples

Display IPv6 BGP routing dampening parameters.

```
<Sysname> display bgp ipv6 routing-table dampening parameter
 Maximum Suppress Time(in second)     : 3069
 Ceiling Value                        : 16000
 Reuse Value                          : 750
```

```
Reach HalfLife Time(in  second)      : 900
Unreach HalfLife Time(in  second)    : 900
Suppress-Limit                       : 2000
```

Table 1-7 Description on the above fields

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Reuse Value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Suppress value

display bgp ipv6 routing-table different-origin-as

Syntax

display bgp ipv6 routing-table different-origin-as

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 routing-table different-origin-as** command to display IPv6 BGP routes originating from different autonomous systems.

Examples

Display routes from different ASs.

```
<Sysname> display bgp ipv6 routing-table different-origin-as

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 222::                                PrefixLen : 64
     NextHop : 122::2                               LocPrf    :
     PrefVal : 0                                    Label     : NULL
     MED     : 0
```

```
    Path/Ogn: 100 ?
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table flap-info

Syntax

display bgp ipv6 routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ipv6-address* [*prefix-length* [**longer-match**]]]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression to be matched, a string of 1 to 80 characters.

as-path-acl-number: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

ipv6-address: IPv6 address of a route to be displayed.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

longer-match: Matches the longest prefix.

Description

Use the **display bgp ipv6 routing-table flap-info** command to display IPv6 BGP route flap statistics.

Examples

Display IPv6 BGP route flap statistics.

```
<Sysname> display bgp ipv6 routing-table flap-info

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network  : 111::                              PrefixLen : 64
     From     : 122::1                             Flaps     : 3
     Duration : 00:13:47                           Reuse     : 00:16:36
     Path/Ogn : 200?
```

Table 1-8 display bgp ipv6 routing-table flap-info command output description

Field	Description
Flaps	Number of flaps
Duration	Flap duration
Reuse	Reuse time of the route

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table peer

Syntax

display bgp ipv6 routing-table peer { *ipv4-address* | *ipv6-address* } { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv4-address: Specifies the IPv4 peer to be displayed.

ipv6-address: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length. The prefix length rangs from 0 to 128.

statistic: Displays route statistics.

Description

Use the **display bgp ipv6 routing-table peer** command to display the routing information advertised to or received from the specified IPv4 or IPv6 BGP peer.

Examples

Display the routing information advertised to the specified BGP peer.

```
<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
 Total Number of Routes: 2

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 20:20::                                PrefixLen : 64
     NextHop : 20:20::20:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i

 *>  Network : 40:40::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
```

```
    Path/Ogn: 300 i
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table regular-expression

Syntax

display bgp ipv6 routing-table regular-expression *as-regular-expression*

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS regular expression, a string of 1 to 80 characters.

Description

Use the **display bgp ipv6 routing-table regular-expression** command to display the routes permitted by the specified AS regular expression.

Examples

Display routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 routing-table regular-expression ^100

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 50:50::                                PrefixLen : 64
     NextHop : 10:10::10:1                           LocPrf    :
     PrefVal : 0                                     Label     : NULL
     MED     : 0
     Path/Ogn: 100 i
```

Refer to Table 1-5 for description on the fields above.

display bgp ipv6 routing-table statistic

Syntax

display bgp ipv6 routing-table statistic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 routing-table statistic** command to display IPv6 BGP routing statistics.

Examples

Display IPv6 BGP routing statistics.

```
<Sysname> display bgp ipv6 routing-table statistic

 Total Number of Routes: 1
```

filter-policy export (IPv6 address family view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

View

IPv6 address family view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of an ACL6 used to match against the destination of routing information. The number is in the range 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol, in the range 1 to 65535. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description

Use the **filter-policy export** command to filter outbound routes using a specified filter.

Use the **undo filter-policy export** command to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

Examples

Reference ACL6 2001 to filter all outbound IPv6 BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

filter-policy import (IPv6 address family view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View

IPv6 address family view

Default Level

2: System level

Parameters

acl6-number: Number of an IPv6 ACL used to match against the destination address field of routing information, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to match against the destination address field of routing information, a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to filter inbound routing information using a specified filter.

Use the **undo filter-policy import** command to cancel filtering inbound routing information.

By default, no inbound routing information is filtered.

Examples

Reference ACL6 2001 to filter all inbound routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import
```

group (IPv6 address family view)

Syntax

group *ipv6-group-name* [**internal** | **external**]

undo group *ipv6-group-name*

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 peer group, a string of 1 to 47 characters.

internal: Creates an IBGP peer group.

external: Creates an EBGP peer group, which can be a group of another sub AS in the confederation.

Description

Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group will be created if neither **internal** nor **external** is selected.

Examples

Create an IBGP peer group named **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] group test
```

import-route (IPv6 address family view)

Syntax

import-route *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View

IPv6 address family view

Default Level

2: System level

Parameters

protocol: Redistributes routes from the specified protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** and **static** at present.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

med-value: Applies the MED value to redistributed routes. The value is in the range 0 to 4294967295. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the incomplete origin attribute.

Examples

Redistribute routes from RIPng 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] import-route ripng 1
```

ipv6-family

Syntax

ipv6-family

undo ipv6-family

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6-family** command to enter IPv6 address family view.

Use the **undo ipv6-family** command to remove all configurations from the view.

IPv4 BGP unicast view is the default.

Examples

Enter IPv6 address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6]
```

network (IPv6 address family view)

Syntax

network *ipv6-address prefix-length* [**short-cut** | **route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length* [**short-cut**]

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address.

prefix-length: Prefix length of the address, in the range 0 to 128.

short-cut: If the keyword is specified for an EBGP route, the route will use the local routing management value rather than that of EBGP routes, so the preference of the route is reduced.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description

Use the **network** command to advertise a network to the IPv6 BGP routing table.

Use the **undo network** command to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

Note that:

- The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

Examples

Advertise the network 2002::/16 into the IPv6 BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

peer advertise-community (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any peer group/peer.

Examples

Advertise the community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

Examples

Advertise the extended community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

number: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

Description

Use the **peer allow-as-loop** command to configure IPv6 BGP to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the times for which it can appear.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number is not allowed to exist in the AS PATH attribute of routes by default.

Examples

Configure the number of times for which the local AS number can appear in the AS PATH of routes from peer 1::1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2
```

peer as-number (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **as-number** *as-number*

undo peer *ipv6-group-name* **as-number**

undo peer *ipv6-address*

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group, in the range 1 to 65535.

Description

Use the **peer as-number** command to specify a peer/peer group with an AS number.

Use the **undo peer as-number** command to delete a peer group.

Use the **undo peer** command to delete a peer.

By default, no peer/peer group is specified.

Examples

Specify peer group **test** in AS 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test as-number 200
```

peer as-path-acl (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-path-acl-number: Number of an AS path ACL, in the range 1 to 256.

import: Filters incoming routes.

export: Filters outgoing routes.

Description

Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path list is specified for filtering.

Examples

Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.

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

```
[Sysname] ip as-path 3 permit ^200
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

peer capability-advertise route-refresh

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

undo peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer capability-advertise route-refresh** command to enable IPv6 BGP route-refresh.

Use the **undo peer capability-advertise route-refresh** command to disable the function.

By default, route-refresh is enabled.

Examples

Disable route-refresh of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

peer connect-interface (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **connect-interface** *interface-type interface-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **connect-interface**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interface-type interface-number: Specifies the type and name of the interface.

Description

Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to an IPv6 BGP peer or peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the IPv6 BGP peer/peer group as the source interface for establishing a TCP connection.

Note that:

To establish multiple BGP connections to a BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples

Specify loopback 0 as the source interface for routing updates to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 connect-interface loopback 0
```

peer default-route-advertise

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Route-policy name, a string of 1 to 19 characters.

Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

Examples

Advertise a default route to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

peer description (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **description** *description-text*

undo peer { *ipv6-group-name* | *ipv6-address* } **description**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description

Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

Examples

Configure the description for the peer group **test** as **ISP1**.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
```

```
[Sysname-bgp-af-ipv6] peer test description ISP1
```

peer ebgp-max-hop (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

hop-count: Maximum hop count, in the range 1 to 255. By default, the value is 64.

Description

Use the **peer ebgp-max-hop** command to allow establishing the EBGP connection to a peer/peer group indirectly connected.

Use the **undo peer ebgp-max-hop** command to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the EBGP connection.

Examples

Allow establishing the EBGP connection with the peer group **test** on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

peer fake-as (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **fake-as** *as-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **fake-as**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description

Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Examples

Configure a fake AS number of 200 for the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

peer filter-policy (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** *acl6-number* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** [*acl6-number*] { **import** | **export** }

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

acl6-number: IPv6 ACL number, in the range 2000 to 3999.

import: Applies the filter-policy to routes received from the peer/peer group.

export: Applies the filter-policy to routes advertised to the peer/peer group.

Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Examples

Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 address family view)

Syntax

peer { *ipv4-address* | *ipv6-address* } **group** *group-name* [**as-number** *as-number*]

undo peer *ipv6-address* **group** *group-name*

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-number: Specifies the AS number of the peer/peer group, in the range 1 to 65535.

Description

Use the **peer group** command to add a peer to a configured peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

Examples

Create a peer group named **test** and add the peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

peer ignore (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **ignore**

undo peer { *ipv6-group-name* | *ipv6-address* } **ignore**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer ignore** command to terminate the session to a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, this means all the sessions with the peer group will be tore down.

Examples

Terminate the session with peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

peer ipv6-prefix

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

import: Applies the filtering policy to routes received from the specified peer/peer group.

export: Applies the filtering policy to routes advertised to the specified peer/peer group.

Description

Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list is specified for filtering.

Examples

Reference the IPv6 prefix list **list 1** to filter routes outgoing to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ipv6-prefix list1 export
```

peer keep-all-routes (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer keep-all-routes** command to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples

Save routing information from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

peer log-change (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **log-change**

undo peer { *ipv6-group-name* | *ipv6-address* } **log-change**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer log-change** command to enable the logging of session state and event information of a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples

Enable the logging of session state and event information of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

peer next-hop-local (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

undo peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer next-hop-local** command to configure the next hop of routes advertised to a peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, the system sets the next hop of routes advertised to an EBGP peer/peer group to the local router, but does not set for routes outgoing to an IBGP peer/peer group.

Examples

Set the next hop of routes advertised to IBGP peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] peer test next-hop-local
```

peer preferred-value (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*

undo peer { *ipv6-group-name* | *ipv6-address* } **preferred-value**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

value: Preferred value, in the range 0 to 65535.

Description

Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

Note that:

If you both reference a routing policy and use the command **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value* to set a preferred value for routes from a peer, the routing policy sets a non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the command **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** } in this document, and the command **apply preferred-value** *preferred-value* in *Routing Policy Commands* of the *IP Routing Volume*.

Examples

Configure the preferred value as 50 for routes from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

undo peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer public-as-only** command to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

Examples

Configure BGP updates sent to the peer 1:2::3:4 to not carry private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients**, **reflector cluster-id**.

Examples

Configure the local device as a route reflector and specify the peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test
[Sysname-bgp-af-ipv6] peer test reflect-client
```

peer route-limit (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit** *prefix-number* [{ **alert-only** | **reconnect** *reconnect-time* } | *percentage*] *

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit**

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

prefix number: Specifies the upper limit of prefixes that can be received from the peer or peer group. The limit varies with devices.. When the received prefixes from the peer/peer group reach the specified upper limit, the router will disconnect from the peer/peer group.

alert-only: When the received prefixes from the peer/peer group reach the specified upper limit, the router will display alarm messages rather than disconnect from the peer/peer group.

reconnect-time: Interval for the router to reconnect to the peer/peer group. The argument has no default. It ranges from 1 to 65535 seconds.

percentage: Specifies a percentage value. If the percentage of received routes to the upper limit reaches the value, the router will generate alarm messages. The default is 75. The value is in the range 1 to 100.

Description

Use the **peer route-limit** command to set the maximum number of prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

The router will end the peer relation when the number of address prefixes received for the peer exceeds the limit.

Examples

Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 100
```

peer route-policy (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

View

IPv6 address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Specifies route-policy name, a string of 1 to 19 characters.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes sent to the peer (group).

Description

Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is specified for the peer (group).

Use of the **peer route-policy** command does not apply the **if-match interface** clause defined in the routing policy. Refer to *Routing Policy Commands* in the *IP Routing Volume* for related information.

Examples

Apply the routing policy test-policy to routes received from the peer group test.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

peer route-update-interval (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **route-update-interval** *interval*

undo peer { *ipv6-group-name* | *ipv6-address* } **route-update-interval**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interval: Specifies the minimum interval for sending the same update to a peer (group) from 5 to 600 seconds.

Description

Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default.

By default, the interval is 15 seconds for the IBGP peer, and 30 seconds for the EBGP peer.

Examples

Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

peer substitute-as (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **substitute-as**

undo peer { *ipv6-group-name* | *ipv6-address* } **substitute-as**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use the **peer substitute-as** command to substitute the local AS number for the AS number of a peer/peer group in the AS_PATH attribute.

Use the **undo peer substitute-as** command to remove the configuration.

The substitution is not configured by default.

Examples

Substitute the local AS number for the AS number of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

peer timer (IPv6 address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *ipv6-group-name* | *ipv6-address* } **timer**

View

IPv6 address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

keepalive: Specifies the keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Specifies the holdtime in seconds, ranging from 3 to 65535.

Description

Use the **peer timer** command to configure keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

keepalive interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples

Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keepalive 60 hold 180
```

preference (IPv6 address family view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

IPv6 address family view

Default Level

2: System level

Parameters

external-preference: Preference of EBGP route learned from an EBGP peer, in the range 1 to 255.

internal-preference: Preference of IBGP route learned from an IBGP peer, in the range 1 to 255.

local-preference: Preference of IPv6 BGP local route, in the range 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. The routing policy can set a preference for routes passing it. The default value applies to the routes filtered out.

Description

Use the **preference** command to configure preferences for EBGP, IBGP, and local routes.

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

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130 respectively.

Examples

Configure preferences for EBGP, IBGP, and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] preference 20 20 200
```

reflect between-clients (IPv6 address family view)

Syntax

reflect between-clients

undo reflect between-clients

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, it is recommended to disable route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id**, **peer reflect-client**.

Examples

Enable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflect between-clients
```

reflector cluster-id (IPv6 address family view)

Syntax

reflector cluster-id *cluster-id*

undo reflector cluster-id

View

IPv6 address family view

Default Level

2: System level

Parameters

cluster-id: Specifies the cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

Examples

Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

refresh bgp ipv6

Syntax

refresh bgp ipv6 { *ipv4-address* | *ipv6-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

ipv4-address: Soft-resets the connection with an IPv4 BGP peer.

ipv6-address: Soft-resets the connection with an IPv6 BGP peer.

all: Soft-resets all IPv6 BGP connections.

external: Soft-resets EBGP connections.

group *ipv6-group-name*: Soft-resets connections with a peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IBGP connections.

export: Performs soft reset in outbound direction.

import: Performs soft reset in inbound direction.

Description

Use the **refresh bgp ipv6** command to soft reset specified IPv4/IPv6 BGP connections. With this feature, you can refresh the IPv4/IPv6 BGP routing table and apply a new available policy without tearing down BGP connections.

To perform IPv4/IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

Examples

Soft reset inbound IPv6 BGP connections.

```
<Sysname> refresh bgp ipv6 all import
```

reset bgp ipv6

Syntax

reset bgp ipv6 { *as-number* | *ipv4-address* | *ipv6-address* [**flap-info**] | **all** | **group** *group-name* | **external** | **internal** }

View

User view

Default Level

1: Monitor level

Parameters

as-number: Resets the IPv6 BGP connections to peers in the specified AS.

ipv4-address: Resets the connection to the specified IPv4 BGP peer.

ipv6-address: Resets the connection to the specified IPv6 BGP peer.

flap-info: Clears the history information of routing flaps.

all: Resets all IPv6 BGP connections.

group *group-name*: Resets the connections to the specified IPv6 BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description

Use the **reset bgp ipv6** command to reset specified IPv4/IPv6 BGP connections.

Examples

Reset all the IPv6 BGP connections.

```
<Sysname> reset bgp ipv6 all
```

reset bgp ipv6 dampening

Syntax

reset bgp ipv6 dampening [*ipv6-address prefix-length*]

View

User view

Default Level

1: Monitor level

Parameters

ipv6-address: IPv6 address

prefix-length: Prefix length of the address, in the range 0 to 128.

Description

Use the **reset bgp ipv6 dampening** command to clear dampened IPv6 BGP route information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all dampened IPv6 BGP route information will be cleared.

Examples

Clear the dampened information of routes to 2345::/64 and release suppressed routes.

```
<Sysname> reset bgp ipv6 dampening 2345:: 64
```

reset bgp ipv6 flap-info

Syntax

reset bgp ipv6 flap-info [*ipv6-address/prefix-length* | **regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number*]

View

User view

Default Level

1: Monitor level

Parameters

ipv6-address: Clears the flap statistics for the specified IPv6 address.

prefix-length: Prefix length of the address, in the range 1 to 128.

as-path-regexp: Clears the flap statistics for routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics for routes matching the AS path ACL. The number is in the range 1 to 256.

Description

Use the **reset bgp ipv6 flap-info** command to clear IPv6 routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples

Clear the flap statistics of the routes matching AS path ACL 10.

```
<Sysname> system-view
[Sysname] ip as-path 10 permit ^100.*200$
[Sysname] quit
<Sysname> reset bgp ipv6 flap-info as-path-acl 10
```

router-id

Syntax

router-id *router-id*

undo router-id

View

BGP view

Default Level

2: System level

Parameters

router-id: Router ID in IP address format.

Description

Use the **router-id** command to specify a router ID for the router.

Use the **undo router-id** command to remove a router ID.

To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.

A router ID can be configured manually. If not, the system will select a router ID automatically from the current interfaces' IPv4 addresses. The selection sequence is the highest IPv4 address of Loopback interfaces' addresses, then the highest IPv4 address of physical interfaces' addresses if no Loopback interfaces are configured.

Only when the interface with the router ID is removed or the manually configured router ID is removed, will the system select another Router ID. To improve network reliability, it is recommended to configure the IPv4 address of a loopback interface as the router ID.

Examples

Specify the router ID of the router as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

synchronization (IPv6 address family view)

Syntax

synchronization

undo synchronization

View

IPv6 address family view

Default Level

2: System level

Parameters

None

Description

Use the **synchronization** command to enable the synchronization between IPv6 BGP and IGP.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

By default, upon receiving an IPv6 IBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the IBGP route can be advertised to EBGP peers only when the route is also advertised by the IGP.

Note

Currently, the system does not support synchronization. Therefore, the configuration of this command does not actually take effect.

Examples

Enable the route synchronization between IPv6 BGP and IGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] synchronization
```

timer (IPv6 address family view)

Syntax

timer keepalive *keepalive* **hold** *holdtime*

undo timer

View

IPv6 address family view

Default Level

2: System level

Parameters

keepalive: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description

Use the **timer** command to specify IPv6 BGP keepalive interval and holdtime interval.

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

By default, the keepalive and holdtime intervals are 60s and 180s respectively.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the IPv6 BGP peers. It becomes valid only after the corresponding IPv6 BGP connections are reset.

Related commands: **peer timer**.

Examples

Configure keepalive interval and holdtime interval as 60 and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] timer keepalive 60 hold 180
```

Table of Contents

1 Route Policy Configuration Commands

Note

- The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.
- The common configuration commands of route policy are applicable to both IPv4 and IPv6.
- EA boards (such as LSQ1GP12EA and LSQ1TGX1EA) do not support IPv6 features.

Common Route Policy Configuration Commands

apply as-path

Syntax

apply as-path *as-number*&<1-10> [**replace**]

undo apply as-path

View

Route policy view

Default Level

2: System level

Parameters

as-number: Autonomous system number, in the range of 1 to 65535.

&<1-10>: Indicates you can enter up to 10 AS numbers.

replace: Replaces the original AS numbers.

Description

Use the **apply as-path** command to apply the specified AS numbers to BGP routes.

Use the **undo apply as-path** command to remove the clause configuration.

No AS_PATH attribute is set by default.

With the **replace** keyword included, the **apply as-path** command replaces the original AS_PATH attribute with the specified AS numbers. Without the **replace** keyword, this command adds the specified AS numbers before the original AS_PATH attribute.

Examples

Configure node 10 in permit mode of route policy **policy1**: add AS number 200 before the original AS_PATH attribute of BGP routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply as-path 200
```

apply comm-list delete

Syntax

apply comm-list *comm-list-number* **delete**

undo apply comm-list

View

Route policy view

Default Level

2: System level

Parameters

comm-list-number: Community list number. A basic community list number ranges from 1 to 99. A advanced community list number ranges from 100 to 199.

Description

Use the **apply comm-list delete** command to remove the community attributes specified by the community list from BGP routing information.

Use the **undo apply comm-list** command to remove the clause configuration.

No community attributes are removed from BGP routing information by default.

Examples

Configure node 10 in permit mode of route policy **policy1**: remove the community attributes specified in community list 1 from the BGP routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

apply community

Syntax

apply community { **none** | **additive** | { *community-number*&<1-16> | *aa:nn*&<1-16> | **internet** | **no-export-subconfed** | **no-export | no-advertise** } ***** [**additive**] }

undo apply community

View

Route policy view

Default Level

2: System level

Parameters

none: Removes the community attributes of BGP routes.

community-number: Community sequence number, in the range 1 to 4294967295.

aa:nn: Community number; both aa and nn are in the range 0 to 65535.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

internet: Sets the **internet** community attribute for BGP routes. Routes with this attribute can be advertised to all BGP peers.

no-export-subconfed: Sets the **no-export-subconfed** community attribute for BGP routes. Routes with this attribute cannot be advertised out the sub autonomous system.

no-advertise: Sets the **no-advertise** community attribute for BGP routes. Routes with this attribute cannot be advertised to any peers.

no-export: Sets the **no-export** community attribute for BGP routes. Routes with this attribute cannot be advertised out the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

additive: Adds the specified community attribute to the original community attribute of BGP routes.

Description

Use the **apply community** command to set the specified community attribute for BGP routes.

Use the **undo apply community** command to remove the apply clause.

No community attribute is set for BGP routes by default.

Related commands: **ip community-list**, **if-match community**, **route-policy**.

Examples

Configure node 16 in permit mode of route policy **setcommunity**: Set the no-export community attribute for BGP routes matching AS-PATH list 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

apply cost

Syntax

apply cost [**+** | **-**] *value*

undo apply cost

View

Route policy view

Default Level

2: System level

Parameters

+: Increases a cost value.

+: Decreases a cost value.

cost: Cost in the range 0 to 4294967295.

Description

Use the **apply cost** command to set a cost for routing information.

Use the **undo apply cost** command to remove the clause configuration.

No cost is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply origin**, **apply tag**.

Examples

Create routing policy **policy1** with node 10, matching mode as permit. If a route matches the outbound interface VLAN-interface 10, set the cost for the route to 120.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 10
[Sysname-route-policy] apply cost 120
```

apply cost-type

Syntax

apply cost-type { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

View

Route policy view

Default Level

2: System level

Parameters

external: IS-IS external route.

internal: IS-IS internal route.

type-1: Type-1 external route of OSPF.

type-2: Type-2 external route of OSPF.

Description

Use the **apply cost-type** command to set a cost type for routing information.

Use the **undo apply cost-type** command to remove the clause configuration.

No cost type is set for routing information by default.

Examples

Create node 10 in permit mode of route policy **policy1**: If a route has a tag of 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```

apply extcommunity

Syntax

apply extcommunity { **rt** *route-target* }&<1-16> [**additive**]

undo apply extcommunity

View

Route policy view

Default Level

2: System level

Parameters

rt *route-target*: Sets the route target extended community attribute, which is a string of 3 to 21 characters. A *route-target* has two forms:

16-bit AS number: 32-bit self-defined number, for example, 101:3;

32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

additive: Adds the specified attribute to the original RT community attribute.

Description

Use the **apply extcommunity** command to apply the specified RT extended community attribute to BGP routes.

Use the **undo apply extcommunity** command to remove the clause configuration.

No RT extended community attribute is set for BGP routing information by default.

Examples

Configure node 10 in permit mode of route policy **policy1**: If a BGP route matches AS-PATH list 1, add the RT extended community attribute 100:2 to the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

apply isis

Syntax

apply isis { **level-1** | **level-1-2** | **level-2** }

undo apply isis

View

Route policy view

Default Level

2: System level

Parameters

level-1: Redistributes routes into IS-IS level-1.

level-2: Redistributes routes into IS-IS level-2.

level-1-2: Redistributes routes into both IS-IS level-1 and level-2.

Description

Use the **apply isis** command to redistribute routes into a specified ISIS level.

Use the **undo apply isis** command to remove the clause configuration.

No IS-IS level is set by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1**: If a route has a tag of 8, redistribute the route to IS-IS level-2.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

apply local-preference

Syntax

apply local-preference *preference*

undo apply local-preference

View

Route policy view

Default Level

2: System level

Parameters

preference: BGP local preference, in the range 0 to 4294967295.

Description

Use the **apply local-preference** command to set the specified local preference for BGP routes.

Use the **undo apply local-preference** command to remove the clause configuration.

No local preference is set for BGP routing information by default.

Related commands: **route-policy**.

Examples

Configure node 10 in permit mode of route policy **policy1**: If a route matches AS-PATH list 1, set a local preference of 130 for the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

apply mpls-label

Syntax

apply mpls-label

undo apply mpls-label

View

Route policy view

Default Level

2: System level

Parameters

None

Description

Use the **apply mpls-label** command to set MPLS labels for routing information.

Use the **undo apply mpls-label** command to remove the clause configuration.

No MPLS label is set for routing information by default.

If MPLS labels failed to apply, the routing information can not be advertised.

Examples

Configure node 10 in permit mode of route policy **policy1**: If routing information matches AS-PATH list 1, set MPLS labels for it.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply mpls-label
```

apply origin

Syntax

apply origin { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

View

Route policy view

Default Level

2: System level

Parameters

igp: Sets the origin attribute of BGP routing information to IGP.

egp: Sets the origin attrubute of BGP routing information to EGP.

as-number: Autonomous system number for EGP routes, in the range of 1 to 65535.

incomplete: Sets the origin attribute of BGP routing information to unknown.

Description

Use the **apply origin** command to set the specified origin attribute for BGP routes.

Use the **undo apply origin** command to remove the clause configuration.

No origin attribute is set for BGP routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1**: If BGP routing information matches AS-PATH list 1, set the origin attribute of the routing information to IGP.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply origin igp
```

apply preference

Syntax

apply preference *preference*

undo apply preference

View

Route policy view

Default Level

2: System level

Parameters

preference: Routing protocol preference, in the range of 1 to 255.

Description

Use the **apply preference** command to set a preference for a routing protocol.

Use the **undo apply preference** command to remove the clause configuration.

No preference is set for a routing protocol by default.

If you have set preferences for routing protocols with the **preference** command, using the **apply preference** command will set a new preference for the matching routing protocol. Non-matching routing protocols still use the preferences set by the **preference** command.

Examples

Configure node 10 in permit mode of route policy **policy1**: Set the preference for OSPF external routes to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1or2
[Sysname-route-policy] apply preference 90
```

apply preferred-value

Syntax

apply preferred-value *preferred-value*

undo apply preferred-value

View

Route policy view

Default Level

2: System level

Parameters

preferred-value: Preferred value, in the range of 0 to 65535.

Description

Use the **apply preferred-value** command to set a preferred value for BGP routes.

Use the **undo apply preferred-value** command to remove the clause configuration.

No preferred value is set for BGP routes by default.

Examples

Configure node 10 in permit mode of route policy **policy1**: Set a preferred value of 66 for BGP routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
```

```
[Sysname-route-policy] apply preferred-value 66
```

apply tag

Syntax

apply tag *value*

undo apply tag

View

Route policy view

Default Level

2: System level

Parameters

value: Tag value, in the range 0 to 4294967295.

Description

Use the **apply tag** command to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use the **undo apply tag** command to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin**.

Examples

Configure node 10 in permit mode of route policy **policy1**: set a tag of 100 for OSPF external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100
```

display ip as-path

Syntax

display ip as-path [*as-path-number*]

View

Any view

Default Level

1: Monitor level

Parameters

as-path-number: AS-PATH list number, in the range of 1 to 256.

Description

Use the **display ip as-path** command to display BGP AS-PATH list information.

Information about all BGP AS-PATH lists will be displayed if no *as-path-number* is specified.

Related commands: **ip as-path**, **if-match as-path**, **apply as-path**.

Examples

Display the information of BGP AS-PATH list 1.

```
<Sysname> display ip as-path 1
ListID    Mode      Expression
1         permit    2
```

Table 1-1 display ip as-path command output description

Field	Description
ListID	AS-PATH list ID
Mode	Matching mode: permit, deny
Expression	Regular expression for matching

display ip community-list

Syntax

display ip community-list [*basic-community-list-number* | *adv-community-list-number*]

View

Any view

Default Level

1: Monitor level

Parameters

basic-community-list-number: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

Description

Use the **display ip community-list** command to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list**, **if-match community**, **apply community**.

Examples

Display the information of the BGP community list 1.

```
<Sysname> display ip community-list 1
Community List Number 1
         permit  1:1 1:2 2:2
```

display ip extcommunity-list

Syntax

display ip extcommunity-list [*ext-comm-list-number*]

View

Any view

Default Level

1: Monitor level

Parameters

ext-comm-list-number: Extended community list number, in the range of 1 to 199.

Description

Use the **display ip extcommunity-list** command to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, **apply extcommunity**.

Examples

Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
         permit rt : 9:6
```

display route-policy

Syntax

display route-policy [*route-policy-name*]

View

Any view

Default Level

1: Monitor level

Parameters

route-policy-name: Route policy name, a string of 1 to 19 characters.

Description

Use the **display route-policy** command to display route policy information.

All route policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy**.

Examples

Display the information of route policy 1.

```
<Sysname> display route-policy policy1
Route-policy : policy1
  permit : 10
        if-match ip-prefix abc
        apply cost 120
```

Table 1-2 display route-policy command output description.

Field	Description
Route-policy	Route policy name
Permit	Match mode of route policy node 10
if-match ip-prefix abc	Match criterion
apply cost 120	If the match criterion is satisfied, set a cost of 120 for routing information.

if-match as-path

Syntax

if-match as-path *as-path-number*&<1-16>

undo if-match as-path [*as-path-number*&<1-16>

View

Route policy view

Default Level

2: System level

Parameters

as-path-number: AS path list number, in the range of 1 to 256.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use the **if-match as-path** command to specify AS-PATH list(s) for matching against the AS path attribute of BGP routing information.

Use the **undo if-match as-path** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**, **ip as-path-acl**.

Examples

Define AS-PATH list 2, allowing BGP routing information containing AS number 200 or 300 to pass. Configure node 10 in permit mode of route policy **test**: specify AS-PATH list 2 for matching.

```
<Sysname> system-view
[Sysname] ip as-path 2 permit _*200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match as-path 2
```

if-match community

Syntax

if-match community { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

undo if-match community [*basic-community-list-number* | *adv-community-list-number*]&<1-16>

View

Route policy view

Default Level

2: System level

Parameters

basic-community-list-number: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

whole-match: Exactly matches the specified community list(s).

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use the **if-match community** command to specify community list(s) for matching against the community attribute of BGP routing information.

Use the **undo if-match community** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**, **ip community-list**.

Examples

Define community list 1, allowing BGP routing information with community number 100 or 200 to pass. Then configure node 10 in permit mode of route policy **test**: specify community-list 1 for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

if-match cost

Syntax

if-match cost *value*

undo if-match cost

View

Route policy view

Default Level

2: System level

Parameters

cost: Cost in the range 0 to 4294967295.

Description

Use the **if-match cost** command to match routing information having the specified cost.

Use the **undo if-match cost** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost, apply local-preference**, **apply origin**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1**: define an if-match clause to permit routing information with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

if-match extcommunity

Syntax

if-match extcommunity *ext-comm-list-number*&<1-16>

undo if-match extcommunity [*ext-comm-list-number*&<1-16>]

View

Route policy view

Default Level

2: System level

Parameters

ext-comm-list-number: Extended community list number, in the range of 1 to 199.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use the **if-match extcommunity** command to specify extended community list(s) for matching against the extended community attribute of BGP routing information.

Use the **undo if-match extcommunity** command to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in permit mode of route policy **policy1** to match BGP routing information to extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy] if-match extcommunity 100 150
```

if-match interface

Syntax

if-match interface { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

View

Route policy view

Default Level

2: System level

Parameters

interface-type: Interface type

interface-number: Interface number

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use the **if-match interface** command to specify interface(s) for matching against the outbound interface of routing information.

Use the **undo if-match interface** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1** to permit routing information with the outbound interface as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 1
```

if-match mpls-label

Syntax

if-match mpls-label

undo if-match mpls-label

View

Route policy view

Default Level

2: System level

Parameters

None

Description

Use the **if-match mpls-label** command to specify the MPLS label match criterion.

Use the **undo if-match mpls-label** command to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in permit mode of route policy **policy1** to match the MPLS labels of routing updates.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match mpls-label
```

if-match route-type

Syntax

if-match route-type { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } *

undo if-match route-type [**internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2**] *

View

Route policy view

Default Level

2: System level

Parameters

internal: Internal routes (OSPF intra-area and inter-area routes).

external-type1: OSPF Type 1 external routes.

external-type2: OSPF Type 2 external routes.

external-type1or2: OSPF Type 1 or 2 external routes.

is-is-level-1: IS-IS Level-1 routes.

is-is-level-2: IS-IS Level-2 routes.

nssa-external-type1: OSPF NSSA Type 1 external routes.

nssa-external-type2: OSPF NSSA Type 2 external routes.

nssa-external-type1or2: OSPF NSSA Type 1 or 2 external routes.

Description

Use the **if-match route-type** command to configure a route type match criterion.

Use the **undo if-match route-type** command to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in permit mode of route policy **policy1** to match OSPF internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

if-match tag

Syntax

if-match tag *value*

undo if-match tag

View

Route policy view

Default Level

2: System level

Parameters

value: Specifies a tag from 0 to 4294967295.

Description

Use the **if-match tag** command to match routing information having the specified tag.

Use the **undo if-match tag** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1** to permit RIP, OSPF and IS-IS routing information with a tag of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
```

ip as-path

Syntax

ip as-path *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number*

View

System view

Default Level

2: System level

Parameters

as-path-number: AS-PATH list number, in the range of 1 to 256.

deny: Specifies the matching mode for the AS-PATH list as deny.

permit: Specifies the matching mode for the AS-PATH list as permit.

regular-expression: AS-PATH regular expression, a string of 1 to 50 characters.

BGP routing updates contain the AS path attribute field that identifies the autonomous systems through which the routing information has passed. An AS-PATH regular expression, for example, ^200. *100$, matches the AS path attribute that starts with AS200 and ends with AS100. For the meanings of special characters used in regular expressions, refer to "CLI Display" in *Basic System Configuration* in the *System Volume*.

Description

Use the **ip as-path** command to create an AS-PATH list.

Use the **undo ip as-path** command to remove an AS-PATH list.

No AS-PATH list is created by default.

Examples

Create AS-PATH list 1, permitting routing information whose AS_PATH attribute starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

ip community-list

Syntax

ip community-list *basic-comm-list-num* { **deny** | **permit** } [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

undo ip community-list *basic-comm-list-num* [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list *adv-comm-list-num* { **deny** | **permit** } *regular-expression*

undo ip community-list *adv-comm-list-num* [*regular-expression*]

View

System view

Default Level

2: System level

Parameters

basic-comm-list-num: Basic community list number, in the range 1 to 99.

adv-comm-list-num: Advanced community list number, in the range 100 to 199.

regular-expression: Regular expression of advanced community attribute, a string of 1 to 50 characters.

deny: Specifies the matching mode of the community list as deny.

permit: Specifies the matching mode of the community list as permit.

community-number-list: Community number list, which is in the *community number* or *aa:nn* format; a *community number* is in the range 1 to 4294967295; *aa* and *nn* are in the range 0 to 65535. Up to 16 community numbers can be entered.

internet: Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Routes with this attribute cannot be advertised to other BGP peers.

no-export: Routes with this attribute cannot be advertised out the local AS, or the confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Routes with this attribute cannot be advertised out the local AS, or to other sub ASs in the confederation.

Description

Use the **ip community-list** to define a community list entry.

Use the **undo ip community-list** command to remove a community list or entry.

No community list is defined by default.

Examples

Define basic community list 1 to permit routing information with the **internet** community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

Define advanced community list 100 to permit routing information with the community attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

ip extcommunity-list

Syntax

ip extcommunity-list *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* }&<1-16>

undo ip extcommunity-list *ext-comm-list-number*

View

System view

Default Level

2: System level

Parameters

ext-comm-list-number: Extended community list number, in the range 1 to 199.

permit: Specifies the matching mode for the extended community list as permit.

deny: Specifies the matching mode for the extended community list as deny.

rt *route-target*: Specifies the route target extended community attribute, which is a string of 3 to 21 characters. A *route-target* has two forms:

A 16-bit AS number: a 32-bit self-defined number, for example, 101:3;

A 32-bit IP address: a 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use the **ip extcommunity-list** to define an extended community list entry.

Use the **undo ip extcommunity-list** command to remove an extended community list.

No extended community list is defined by default.

Examples

Define extended community list 1 to permit routing information with RT 200:200.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

route-policy

Syntax

route-policy *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**node** *node-number*]

View

System view

Default Level

2: System level

Parameters

route-policy-name: Route policy name, a string of 1 to 19 characters.

permit: Specifies the matching mode of the route policy node as permit. If a route satisfies all the if-match clauses of the node, it passes the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the route policy.

deny: Specifies the matching mode of the route policy node as deny. If a route satisfies all the if-match clauses of the node, it cannot pass the node and will not go to the next node.

node *node-number*: Node number, in the range 0 to 65535. A node with a smaller number is matched first.

Description

Use the **route-policy** command to create a route policy and a node of it and enter route policy view.

Use the **undo route-policy** command to remove a route policy or a node of it.

No route policy is created by default.

A route policy is used for routing information filtering or policy based routing. It contains several nodes and each node comprises a set of if-match and apply clauses. The if-match clauses define the matching

criteria of the node and the apply clauses define the actions to be taken on packets passing the node. The relation between the if-match clauses of a node is logic AND, namely, all the if-match clauses must be satisfied. The relation between different route policy nodes is logic OR, namely, a packet passing a node passes the route policy.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin**, **apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1** and enter route policy view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy]
```

IPv4 Route Policy Configuration Commands

apply ip-address next-hop

Syntax

apply ip-address next-hop *ip-address*

undo apply ip-address next-hop

View

Route policy view

Default Level

2: System level

Parameters

ip-address: IP address of the next hop.

Description

Use the **apply ip-address next-hop** command to set a next hop for IPv4 routing information.

Use the **undo apply ip-address next-hop** command to remove the clause configuration.

No next hop is set for IPv4 routing information by default.

This command cannot set a next hop for redistributed routes.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply local-preference**, **apply cost**, **apply origin, apply tag**.

Examples

Configure node 10 in permit mode of route policy **policy1** to set next hop 193.1.1.8 for routes matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
```

```
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

display ip ip-prefix

Syntax

display ip ip-prefix [*ip-prefix-name*]

View

Any view

Default Level

1: Monitor level

Parameters

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

Description

Use the **display ip ip-prefix** command to display the statistics of an IPv4 prefix list. If no ip-prefix-name is specified, statistics for all IPv4 prefix lists will be displayed.

Related commands: **ip ip-prefix**.

Examples

Display the statistics of IPv4 prefix list **abc**.

```
<Sysname> display ip ip-prefix abc
Prefix-list abc
Permitted 0
Denied 0
        index: 10              permit  1.0.0.0/11             ge  22  le  32
```

Table 1-3 display ip ip-prefix command output description.

Field	Description
Prefix-list	Name of the IPv4 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
index	Index of the IPv4 prefix list
permit	Matching mode: permit or deny
1.0.0.0/11	IP address and mask
ge	greater-equal, the lower limit
le	less-equal, the higher limit

if-match acl

Syntax

if-match acl *acl-number*

undo if-match acl

View

Route policy view

Default Level

2: System level

Parameters

acl-number: ACL number from 2000 to 3999.

Description

Use the **if-match acl** command to configure an ACL match criterion.

Use the **undo if-match acl** command to remove the match criterion.

No ACL match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples

Configure node 10 of route policy **policy1** to permit routes matching ACL 2000.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match acl 2000
```

if-match ip

Syntax

if-match ip { **next-hop** | **route-source** } { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop | route-source** } [**acl** | **ip-prefix**]

View

Route policy view

Default Level

2: System level

Parameters

next-hop: Matches the next hop of routing information to the filter.

route-source: Matches the source address of routing information to the filter.

acl *acl-number*: Matches an ACL with a number from 2000 to 2999.

ip-prefix *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description

Use the **if-match ip** command to configure a next hop or source address match criterion for IPv4 routes.

Use the **undo if-match ip** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**.

Examples

Configure node 10 of route policy **policy1** to permit routing information whose next hop address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

if-match ip-prefix

Syntax

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix

View

Route policy view

Default Level

2: System level

Parameters

ip-prefix-name: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description

Use the **if-match ip-prefix** command to configure an IP prefix list based match criterion.

Use the **undo if-match ip-prefix** command to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples

Configure node 10 of route policy **policy2** to permit routes whose destination address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy2 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

ip ip-prefix

Syntax

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

View

System view

Default Level

2: System level

Parameters

ip-prefix-name: IPv4 prefix list name, a string of 1 to 19 characters.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an item of the IPv4 prefix list. An index with a smaller number is matched first.

permit: Specifies the matching mode for the IPv4 prefix list item as permit, that is, if a route matches the item, the route passes the IPv4 prefix list without needing to match against the next item; if not, it will match against the next item (supporse the IPv4 prefix list has multiple items configured).

deny: Specifies the matching mode for the IPv4 prefix list item as deny, that is, if a route matches the item, the route neither passes the filter nor matches against the next item; if not, the route will match against the next item (supporse the IPv4 prefix list has multiple items configured).

ip-address mask-length: Specifies an IPv4 prefix and mask length. The *mask-length* is in the range 0 to 32.

min-mask-length, *max-mask-length*: Specifies the prefix range. **greater-equal** means “greater than or equal to” and **less-equal** means “less than or equal to”. The range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32. If only the *min-mask-length* is specified, the prefix length range is [min-mask-length, 32]. If only the *max-mask-length* is specified, the prefix length range is [mask-length, max-mask-length]. If both min-mask-length and max-mask-length are specified, the prefix length range is [min-mask-length, max-mask-length].

Description

Use the **ip ip-prefix** command to configure an IPv4 prefix list or an item of it.

Use the **undo ip ip-prefix** command to remove an IPv4 prefix list or an item of it.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logic OR, namely, if an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and [*min-mask-length, max-mask-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, the IP address must satisfy both of them.

If both *ip-address* and *mask-length* are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

Examples

Define IP prefix list **p1** to permit routes matching network 10.0.192.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

reset ip ip-prefix

Syntax

reset ip ip-prefix [*ip-prefix-name*]

View

User view

Default Level

2: System level

Parameters

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

Description

Use the **reset ip ip-prefix** command to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all IPv4 prefix lists will be cleared.

Examples

Clear the statistics of IPv4 prefix list **abc**.

```
<Sysname> reset ip ip-prefix abc
```

IPv6 Route Policy Configuration Commands

apply ipv6 next-hop

Syntax

apply ipv6 next-hop *ipv6-address*

undo apply ipv6 next-hop

View

Route policy view

Default Level

2: System level

Parameters

ipv6-address: Next hop IPv6 address.

Description

Use the **apply ipv6 next-hop** command to set a next hop for IPv6 routes.

Use the **undo apply ipv6 next-hop** command to remove the clause configuration.

No next hop address is set for IPv6 routing information by default.

This command cannot set a next hop for redistributed routes.

Examples

Configure node 10 of route policy **policy1** to set next hop 3ff3:506::1 for IPv6 routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1
```

display ip ipv6-prefix

Syntax

display ip ipv6-prefix [*ipv6-prefix-name*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

Description

Use the **display ip ipv6-prefix** command to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all IPv6 prefix lists will be displayed.

Examples

Display the statistics of all IPv6 prefix lists.

```
<Sysname> display ip ipv6-prefix
Prefix-list6 abc
Permitted 0
Denied 0
         index:   10            permit  ::/0
         index:   20             permit  ::/1                ge  1   le  128
```

Table 1-4 display ip ipv6-prefix command output description

Field	Description
Prefix-list6	Name of the IPv6 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
Index	Index number of the prefix list
Permit	Matching mode of the item: permit, or deny
::/1	IPv6 address and prefix length for matching

Field	Description
ge	greater-equal, the lower prefix length
Le	less-equal, the upper prefix length

if-match ipv6

Syntax

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** *acl6-number* | **prefix-list** *ipv6-prefix-name* }

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

View

Route policy view

Default Level

2: System level

Parameters

address: Matches the destination address of IPv6 routing information.

next-hop: Matches the next hop of IPv6 routing information.

route-source: Matches the source address of IPv6 routing information.

acl *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

prefix-list *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

Description

Use the **if-match ipv6** command to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use the **undo if-match ipv6** command to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 of route policy **policy1** to permit routing information whose next hop address matches IPv6 prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ipv6 next-hop prefix-list p1
```

ip ipv6-prefix

Syntax

ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

View

System view

Default Level

2: System level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters, for uniquely specifying an IPv6 prefix list.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an IPv6 prefix list item. An item with a smaller *index-number* will be matched first.

permit: Specifies the matching mode for the IPv6 prefix list item as permit, that is, if a route matches the item, it passes the IPv6 prefix list without needing to match against the next item; if not, it will match against the next item (suppose the IPv6 prefix list has multiple items configured).

deny: Specifies the matching mode for the IPv6 prefix list item as deny, that is, if a route matches the item, the route neither passes the filter nor matches against the next item; if not, the route will match against the next item (suppose the IPv6 prefix list has multiple items configured).

ipv6-address prefix-length: Specifies an IPv6 prefix and prefix length. A *prefix-length* is in the range 0 to 128. When specified as :: 0, the arguments matche the default route.

greater-equal *min-prefix-length:* Greater than or equal to the minimum prefix length.

less-equal *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 128. If only the min-prefix-length is specified, the prefix length range is [min-prefix-length, 128]. If only the max-prefix-length is specified, the prefix length range is [prefix-length, max-prefix-length]. If both the min-prefix-length and max-prefix-length are specified, the prefix length range is [min-prefix-length, max-prefix-length].

Description

Use the **ip ipv6-prefix** command to configure an IPv6 prefix list or an item of it.

Use the **undo ip ipv6-prefix** command to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

An IPv6 prefix list may have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between items is logic OR, namely, if a route passes an item of it, the route will pass the IPv6 prefix list.

The IPv6 prefix range is determined by *prefix-length* and [*min-prefix-length, max-prefix-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

Examples

Permit IPv6 addresses with a mask length between 32 bits and 64 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

Deny IPv6 addresses with the prefix being 3FFE:D00::/32, and prefix length being greater than or equal to 32 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc deny 3FEE:D00:: 32 less-equal 128
```

reset ip ipv6-prefix

Syntax

reset ip ipv6-prefix [*ipv6-prefix-name*]

View

User view

Default Level

2: System level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

Description

Use the **reset ip ipv6-prefix** command to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

Examples

Clear the statistics of IPv6 prefix list **abc**.

```
<Sysname> reset ip ipv6-prefix abc
```

IP Multicast Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The IP Multicast Volume is organized as follows:

Features	Description
Multicast Routing and Forwarding	Multicast routing and forwarding refer to some policies that filter RPF routing information for IP multicast support. This document introduces the commands for Multicast Routing and Forwarding configuration.
IGMP	Internet Group Management Protocol (IGMP) is a protocol in the TCP/IP suite responsible for management of IP multicast members. This document introduces the commands for IGMP configuration.
PIM	PIM leverages the unicast routing table created by any unicast routing protocol to provide routing information for IP multicast. This document introduces the commands for PIM configuration.
MSDP	Multicast source discovery protocol (MSDP) describes interconnection mechanism of multiple PIM-SM domains. It is used is to discover multicast source information in other PIM-SM domains. This document introduces the commands for MSDP configuration.
MBGP	As a multicast extension of MP-BGP, MBGP enables BGP to provide routing information for multicast applications. This document introduces the commands for MBGP configuration.
Multicast VPN	Multicast VPN is a technique that implements multicast delivery in MPLS L3VPN networks. This document introduces the commands for Multicast VPN configuration.
IGMP Snooping	Running at the data link layer, IGMP Snooping is a multicast control mechanism on the Layer 2 Ethernet switch and it is used for multicast group management and control. This document introduces the commands for IGMP Snooping configuration.
Multicast VLAN	This document introduces the commands for Multicast VLAN configuration.
IPv6 Multicast Routing and Forwarding	IPv6 multicast routing and forwarding refer to some policies that filter RPF routing information for IPv6 multicast support. This document introduces the commands for IPv6 Multicast Routing and Forwarding configuration.
MLD	MLD is used by an IPv6 router or a Ethernet Switch to discover the presence of multicast listeners on directly-attached subnets. This document introduces the commands for MLD configuration.

Features	Description
IPv6 PIM	IPv6 PIM discovers multicast source and delivers information to the receivers. This document introduces the commands for IPv6 PIM configuration.
IPv6 MBGP	As an IPv6 multicast extension of MP-BGP, IPv6 MBGP enables BGP to provide routing information for IPv6 multicast applications. This document introduces the commands for IPv6 MBGP configuration.
MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. This document introduces the commands for MLD Snooping configuration.
IPv6 Multicast VLAN	This document introduces the commands for IPv6 Multicast VLAN configuration.

Table of Contents

1 Multicast Routing and Forwarding Configuration Commands

Note

The term “router” in this document refers to a router in the generic sense or a Layer 3 switch running an IP multicast routing protocol.

Multicast Routing and Forwarding Configuration Commands

display multicast boundary

Syntax

display multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group address, in the range of 4 to 32. The system default is 32.

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

Description

Use the **display multicast boundary** command to view the multicast boundary information on the specified interface or all interfaces.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.

Related commands: **multicast boundary**.

Examples

View the multicast boundary information on all interfaces in the public network instance.

```
<Sysname> display multicast boundary
Multicast boundary information of VPN-Instance: public net
 Boundary            Interface
 224.1.1.0/24        Vlan1
 239.2.2.0/24        Vlan2
```

Table 1-1 display multicast boundary command output description

Field	Description
Multicast boundary information of VPN-Instance: public net	Multicast boundary for the public network
Boundary	Multicast group corresponding to the multicast boundary
Interface:	Boundary interface corresponding to the multicast boundary

display multicast forwarding-table

Syntax

display multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-number*] * [**port-info**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies the interface by its type and number.

register: Displays forwarding entries of which the incoming interface is the register interface of PIM-SM.

outgoing-interface: Displays forwarding entries of which the outgoing interface is the specified one.

exclude: Displays the forwarding entries of which the outgoing interface list excludes the specified interface.

include: Displays the forwarding entries of which the outgoing interface list includes the specified interface.

match: Specifies the forwarding entries of which the outgoing interface list includes and includes only the specified interface.

statistics: Specifies to display the statistics information of the multicast forwarding table.

slot *slot-number*: Displays forwarding entries of the interface card specified by the slot number. If you do not specify this option, this command will display the multicast forwarding table information of the main processing board.

port-info: Specifies to display Layer 2 port information.

Description

Use the **display multicast forwarding-table** command to view the multicast forwarding table information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.
- Multicast forwarding tables are used to guide multicast forwarding. You can view the forwarding state of multicast traffic by checking the multicast forwarding table.

Related commands: **multicast forwarding-table downstream-limit**, **multicast forwarding-table route-limit**, **display multicast routing-table**.

Examples

View the multicast forwarding table information in the public network instance.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
Total 1 entry

Total 1 entry matched

00001. (172.168.0.2, 227.0.0.1)
     MID: 0, Flags: 0x0:0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface1
     List of 1 outgoing interfaces:
       1: Vlan-interface2
     Matched 19648 packets(20512512 bytes), Wrong If 0 packets
     Forwarded 19648 packets(20512512 bytes)
```

Table 1-2 display multicast forwarding-table command output description

Field	Description
Multicast Forwarding Table of VPN-Instance: public net	Multicast forwarding table for the public network
Total 1 entry	Total number of (S, G) entries in the multicast forwarding table
Total 1 entry matched	Total number of matched (S, G) entries in the multicast forwarding table
00001	Sequence number of the (S, G) entry
(172.168.0.2,227.0.0.1)	An (S, G) entry of the multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has a unique MID
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of (S, G) entries. Major values of this field are described in Table 1-3.
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds
Timeout in	Length of time in which the (S, G) entry will expire, in hours:minutes:seconds
Incoming interface	Incoming interface of the (S, G) entry
List of 1 outgoing interface: 1: Vlan-interface2	Outgoing interface list Interface number: outgoing interface name and number
Matched 19648 packets (20512512 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors
Forwarded 19648 packets (20512512 bytes)	(S, G)-forwarded packets (bytes)

Table 1-3 Major values of the **flags** field

Value	Meaning
0x00000001	Indicates that a register-stop message must be sent
0x00000002	Indicates whether the multicast source corresponding to the (S, G) is active
0x00000004	Indicates a null forwarding entry
0x00000008	Indicates whether the RP is a PIM domain border router
0x00000010	Indicates that a register outgoing interface is available
0x00000400	Identifies an (S, G) entry to be deleted
0x00008000	Indicates that the (S, G) entry is in the smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) has been updated during the smoothing process
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before a new entry is added

Value	Meaning
0x00100000	Indicates that an entry is successfully added

display multicast routing-table

Syntax

display multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays multicast routing entries of which the incoming interface is the specified one.

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

register: Displays multicast routing entries of which the incoming interface is the specified register interface of PIM-SM.

outgoing-interface: Displays multicast routing entries of which the outgoing interface is the specified one.

exclude: Displays routing entries of which the outgoing interface list excludes the specified interface.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

Description

Use the **display multicast routing-table** command to view the multicast routing table information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.
- Multicast routing tables are the basis of multicast forwarding. You can view the establishment state of an (S, G) entry by checking the multicast routing table.

Related commands: **display multicast forwarding-table**.

Examples

View the routing information in the multicast routing table of the public instance.

```
<Sysname> display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry
 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Vlan-interface1
       List of 2 downstream interfaces
           1:  Vlan-interface2
           2:  Vlan-interface3
```

Table 1-4 display multicast routing-table command output description

Field	Description
Multicast routing table of VPN-Instance: public net	Multicast routing table for the public network
Total 1 entry	Total number of (S, G) entries in the multicast routing table
00001	Sequence number of the (S, G) entry
(172.168.0.2, 227.0.0.1)	An (S, G) entry of the multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds
Upstream interface	Upstream interface the (S, G) entry: multicast packets should arrive at this interface
List of 2 downstream interfaces	Downstream interface list: these interfaces need to forward multicast packets

display multicast routing-table static

Syntax

display multicast routing-table [**all-instance** | **vpn-instance** *vpn-instance-name*] **static** [**config**] [*source-address* { *mask-length* | *mask* }]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

config: Displays the configuration information of static routes.

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

Description

Use the **display multicast routing-table static** command to view the information of multicast static routes.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.

Examples

View all the multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static
Multicast Routing Table of VPN-Instance: public net
Routes : 1

 Mroute 10.10.0.0/16
          Interface = Vlan-interface1          RPF Neighbor = 2.2.2.2
          Matched routing protocol = <none>, Route-policy = <none>
          Preference = 1, Order = 1
 Running Configuration = ip rpf-route-static 10.10.0.0 16 2.2.2.2 order 1
```

View the configuration information of multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static config

Multicast Routing Table of VPN-Instance: public net
Routes : 1

 Mroute 10.10.0.0/16,    RPF neighbor = 2.2.2.2
 Matched routing protocol = <none>, Route-policy = <none>
 Preference = 1, Order = 1
```

Table 1-5 display multicast routing-table static command output description

Field	Description
Multicast Routing Table of VPN-Instance: public net	Multicast routing table for the public network
Mroute	Multicast route source address and its mask length
Interface	Outgoing interface to the multicast source

Field	Description
RPF Neighbor	IP address of the RPF neighbor through which the multicast source is reachable
Matched routing protocol	If a protocol is configured, the multicast source address of the route should be the destination address of an entry in unicast routing table.
Route-policy	Routing policy. The multicast source address of the route should match the routing policy.
Preference	Route preference
Order	Sequence number of the route

display multicast rpf-info

Syntax

display multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space..

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

Description

Use the **display multicast rpf-info** command to view the RPF information of a multicast source.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.

Related commands: **display multicast routing-table**, **display multicast forwarding-table**.

Examples

View all the RPF information of multicast source 192.168.1.55 in the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
 RPF information about source 192.168.1.55:
     VPN instance: public net
     RPF interface: Vlan-interface1, RPF neighbor: 10.1.1.1
     Referenced route/mask: 192.168.1.0/24
     Referenced route type: igp
```

```
Route selection rule: preference-preferred
Load splitting rule: disable
```

Table 1-6 display multicast rpf-info command output description

Field	Description
RPF information about source 192.168.1.55	Information of the RPF path to multicast source 192.168.1.55
RPF interface	RPF interface
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Referenced route and its mask length
Referenced route type	Type of the referenced route, which can be any of the following: • igp: unicast route (IGP) • egp: unicast route (BGP) • unicast (direct): unicast route (directly connected) • unicast: other unicast route (such as unicast static route) • mbgp: MBGP route • multicast static: multicast static route
Route selection rule	Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address
Load splitting rule	Status of the load splitting rule (enabled/disabled)

ip rpf-route-static

Syntax

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*] { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*]

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space..

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

protocol: Routing protocol, which can have any of the following values:

- **bgp**: Specifies the BGP protocol.
- **isis**: Specifies the IS-IS protocol.
- **ospf**: Specifies the OSPF protocol.
- **rip**: Specifies the RIP protocol.
- **statitc**: Specifies a static route.

process-id: Process number of the unicast routing protocol, in the range of 1 to 65535. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

policy-name: Name of the multicast route match rule, a case sensitive string of up to 19 characters without any space.

rpf-nbr-address: Specifies an RPF neighbor by the IP address.

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

preference: Route preference, in the range of 1 to 255 and defaulting to 1.

order-number: Match order for routes on the same segment, in the range of 1 to 100.

Description

Use the **ip rpf-route-static** command to configure a multicast static route.

Use the **undo ip rpf-route-static** command to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

Note that:

- If **vpn-instance** is not specified, this configuration takes effect only on the public instance.
- The arguments *source-address* { *mask* | *mask-length* }, *protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these three arguments results in a different configuration.
- In the configuration, you can use the **display multicast routing-table static** command to check whether the multicast static route information contains this configuration. If you find a match, modify the corresponding fields without changing the configuration sequence; otherwise, add a multicast static route.
- When configuring a multicast static route, you can specify an RPF neighbor only by providing its IP address (*rpf-nbr-address*) rather than its interface type and number (*interface-type interface-number*) if the interface type of the RPF neighbor is Ethernet, Layer 3 aggregate, Loopback, RPR, or VLAN-interface.
- Because outgoing interface iteration may fail or the specified interface may be in the down state, the multicast static route configured with this command may fail to take effect. Therefore, we recommend that you use the **display multicast routing-table static** command after you configure a multicast static route to check whether the route has been successfully configured or whether the route has taken effect.

Related commands: **display multicast routing-table static**.

Examples

Configure a multicast static route to the multicast source 10.1.1.1/24, specifying a router with the IP address of 192.168.1.23 as its RPF neighbor.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.1 24 192.168.1.23
```

mtracert

Syntax

mtracert *source-address* [[*last-hop-router-address*] *group-address*]

View

Any view

Default Level

1: Monitor level

Parameters

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

last-hop-router-address: Specifies a last-hop router address, which is the IP address of the local router by default.

Description

Use the **mtracert** command to trace the path down which the multicast traffic flows to the last-hop router.

Note that if the *last-hop-router-address* argument is given in the command to trace the path for a specific (S, G) multicast stream, the interface corresponding to the last-hop router address must be the outgoing interface for the (S, G) entry; otherwise the multicast traceroute will fail.

Examples

Trace the path down which the (6.6.6.6, 225.2.1.1) multicast traffic flows to the last-hop router with an IP address of 5.5.5.8.

```
<Sysname> mtracert 6.6.6.6 5.5.5.8 225.2.1.1
 Type Ctrl+C to quit mtrace facility
 Tracing reverse path of (6.6.6.6, 225.2.1.1) from last-hop router (5.5.5.8) to source via
multicast routing-table

 -1 5.5.5.8
   Incoming interface address: 4.4.4.8
   Previous-hop router address: 4.4.4.7
   Input packet count on incoming interface: 17837
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 8000
   Protocol: PIM
   Forwarding TTL: 0
   Forwarding code: No error

 -2 4.4.4.7
   Incoming interface address: 6.6.6.7
   Previous-hop router address: 0.0.0.0
   Input packet count on incoming interface: 2
   Output packet count on outgoing interface: 259
```

```
Total number of packets for this source-group pair: 8100
Protocol: PIM
Forwarding TTL: 0
Forwarding code: No error
```

Table 1-7 mtracert command output description

Field	Description
(6.6.6.6, 225.2.1.1)	The (S, G) multicast stream for which the forwarding path is being traced
-1 5.5.5.8	The (S, G) outgoing interface address of each hop, starting from the last-hop router
Incoming interface address	The address of the interface on which the (S, G) packets arrive
Previous-hop router address	The IP address of the router from which this router receives packets from this source
Input packet count on incoming interface	The total number of multicast packets received on the incoming interface
Output packet count on outgoing interface	The total number of multicast packets transmitted on the outgoing interface
Total number of packets for this source-group pair	The total number of packets from the specified source forwarded by this router to the specified group
Protocol	The multicast routing protocol in use
Forwarding TTL	The minimum TTL that a packet is required to have before it can be forwarded over the outgoing interface

multicast boundary

Syntax

multicast boundary *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

View

Interface view

Default Level

2: System level

Parameters

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address, in the range of 4 to 32.

all: Specifies to remove all forwarding boundaries configured on the interface.

Description

Use the **multicast boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast boundary** command to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast boundary**.

Examples

Configure VLAN-interface 100 to be the forwarding boundary of multicast group 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast boundary 239.2.0.0 16
```

multicast forwarding-table downstream-limit

Syntax

multicast forwarding-table downstream-limit *limit*

undo multicast forwarding-table downstream-limit

View

System view, VPN instance view

Default Level

2: System level

Parameters

limit: Maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single multicast forwarding entry. The value ranges from 0 to 128.

Description

Use the **multicast forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single entry in the multicast forwarding table.

Use the **undo multicast forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single multicast forwarding entry is the maximum number allowed by the system, namely 128.

The system-allowed maximum number varies with different device models.

Related commands: **display multicast forwarding-table**.

Examples

Set the maximum number of downstream nodes for a single multicast forwarding entry of the public instance to 120.

```
<Sysname> system-view
[Sysname] multicast forwarding-table downstream-limit 120
```

Set the maximum number of downstream nodes for a single multicast forwarding entry of VPN instance mvpn to 60.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast forwarding-table downstream-limit 60
```

multicast forwarding-table route-limit

Syntax

multicast forwarding-table route-limit *limit*

undo multicast forwarding-table route-limit

View

System view, VPN instance view

Default Level

2: System level

Parameters

limit: Maximum number of entries in the multicast forwarding table. The value ranges 0 to 1000.

Description

Use the **multicast forwarding-table route-limit** command to configure the maximum number of entries in the multicast forwarding table.

Use the **undo multicast forwarding-table route-limit** command to restore the maximum number of entries in the multicast forwarding table to the system default.

By default, the maximum number of entries in the multicast forwarding table is the maximum number allowed by the system, namely 1000.

The system-allowed maximum number varies with different device models.

Related commands: **display multicast forwarding-table**.

Examples

Set the maximum number of entries in the multicast forwarding table of the public instance to 200.

```
<Sysname> system-view
[Sysname] multicast forwarding-table route-limit 200
```

Set the maximum number of entries in the multicast forwarding table of VPN instance mvpn to 200.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
```

```
[Sysname-vpn-instance-mvpn] multicast forwarding-table route-limit 200
```

multicast load-splitting

Syntax

multicast load-splitting { **source** | **source-group** }

undo multicast load-splitting

View

System view, VPN instance view

Default Level

2: System level

Parameters

source: Specifies to implement per-source load splitting.

source-group: Specifies to implement per-source and per-group load splitting simultaneously.

Description

Use the **multicast load-splitting** command to enable load splitting of multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

Examples

Enable per-source load splitting of multicast traffic in the public instance.

```
<Sysname> system-view
[Sysname] multicast load-splitting source
```

Enable per-source load splitting of multicast traffic in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast load-splitting source
```

multicast longest-match

Syntax

multicast longest-match

undo multicast longest-match

View

System view, VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **multicast longest-match** command to configure the device to select the RPF route based on the longest match principle, namely to select the route with the longest mask as the RPF route.

Use the **undo multicast longest-match** command to restore the default.

By default, the device selects the route with the highest priority as the RPF route.

Examples

Configure the device to select the RPF route based on the longest match principle in the public instance.

```
<Sysname> system-view
[Sysname] multicast longest-match
```

Configure route selection based on the longest match in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast longest-match
```

multicast routing-enable

Syntax

multicast routing-enable

undo multicast routing-enable

View

System view, VPN instance view

Default Level

2: System level

Parameters

None

Description

Use the **multicast routing-enable** command to enable IP multicast routing.

Use the **undo multicast routing-enable** command to disable IP multicast routing.

IP multicast routing is disabled by default.

Note that:

- You must enable IP multicast routing in the public instance or VPN instance before you can carry out other Layer 3 multicast commands in the corresponding instance.
- The device does not forward any multicast packets before IP multicast routing is enabled.

Examples

Enable IP multicast routing in the public instance.

```
<Sysname> system-view
[Sysname] multicast routing-enable
```

Enable IP multicast routing in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
```

reset multicast forwarding-table

Syntax

reset multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Specifies to clear multicast forwarding entries of which the incoming interface is the specified one.

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

register: Specifies o clear multicast forwarding entries of which the incoming interface is the specified register interface of PIM-SM..

all: Specifies to clear all the forwarding entries from the multicast forwarding table.

Description

Use the **reset multicast forwarding-table** command to clear the multicast forwarding table information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command clears the forwarding table information on the public instance.
- When a forwarding entry is deleted from the multicast forwarding table, the corresponding route entry is also deleted from the multicast routing table.

Related commands: **reset multicast routing-table**, **display multicast routing-table**, **display multicast forwarding-table**.

Examples

Clear the multicast forwarding entries related to multicast group 225.5.4.3 from the multicast forwarding table of the public instance.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

Clear the multicast forwarding entries related to multicast group 226.1.2.3 from the multicast forwarding table of VPN instance mvpn.

```
<Sysname> reset multicast vpn-instance mvpn forwarding-table 226.1.2.3
```

reset multicast routing-table

Syntax

reset multicast [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Specifies to clear the routing entries of which the incoming interface is the specified one..

register: Specifies to clear the routing entries of which the incoming interface is the specified register interface of PIM-SM..

all: Specifies to clear all the routing entries from the multicast routing table.

Description

Use the **reset multicast routing-table** command to clear multicast routing entries from the multicast routing table.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public instance.
- When a route entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

Related commands: **reset multicast forwarding-table**, **display multicast routing-table**, **display multicast forwarding-table**.

Examples

Clear the route entries related to multicast group 225.5.4.3 from the multicast routing table of the public instance.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

Clear the route entries related to multicast group 226.1.2.3 from the multicast routing table of VPN instance mvpn.

```
<Sysname> reset multicast vpn-instance mvpn routing-table 226.1.2.3
```

Table of Contents

1 IGMP Configuration Commands

Note

The term "router" in this document refers to a router in a generic sense or a Layer 3 switch running an IP routing protocol.

IGMP Configuration Commands

display igmp group

Syntax

display igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all nstances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

interface *interface-type interface-number*: Displays the IGMP multicast group information about a particular interface.

static: Displays the information of statically joined IGMP multicast groups.

verbose: Displays the detailed information of IGMP multicast groups.

Description

Use the **display igmp group** command to view IGMP multicast group information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.
- If you do not specify *group-address*, this command will display the IGMP information of all the multicast groups.

- If you do not specify *interface-type interface-number*, this command will display the IGMP multicast group information on all the interfaces.
- If you do not specify the **static** keyword, this command will display the detailed information about the dynamically joined IGMP multicast groups.

Examples

Display the information about dynamically joined IGMP multicast groups on all interfaces in the public instance.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 Vlan-interface1(20.20.20.20):
  Total 3 IGMP Groups reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       20.20.20.20     00:02:04    00:01:15
   225.1.1.3       20.20.20.20     00:02:04    00:01:15
   225.1.1.2       20.20.20.20     00:02:04    00:01:17
```

Display the detailed information of multicast group 225.1.1.1 in the public instance.

```
<Sysname> display igmp group 225.1.1.1 verbose
Interface group report information of VPN-Instance: public net
 Vlan-interface1(10.10.1.20):
  Total 1 IGMP Groups reported
   Group: 225.1.1.1
     Uptime: 00:00:34
     Expires: 00:00:40
     Last reporter: 10.10.1.10
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Version1-host-present-timer-expiry: off
```

Table 1-1 display igmp group command output description

Field	Description
Interface group report information of VPN-Instance: public net	IGMP multicast group information on a public network interface
Total 1 IGMP Groups reported	One IGMP multicast group was reported.
Group	Multicast group address
Uptime	Length of time since the multicast group was reported
Expires	Remaining time of the multicast group, where “off” means that the multicast group never times out
Last reporter	Address of the last host that reported its membership for this multicast group
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer, where “off” means that the timer never expires

Field	Description
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where “off” means that the timer never expires

display igmp group port-info

Syntax

display igmp group port-info [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command will display the Layer 2 port information of IGMP multicast groups in all VLANs.

slot *slot-number*: Displays the Layer 2 port information about IGMP multicast groups on the specified card. If you do not specify a slot number, this command will display the Layer 2 port information about IGMP multicast groups on the SRPU.

verbose: Displays the detailed information about Layer 2 ports of IGMP multicast groups.

Description

Use the **display igmp group port-info** command to view Layer 2 port information of IGMP multicast groups.

Examples

View detailed Layer 2 ports information of IGMP multicast groups.

```
<Sysname> display igmp group port-info 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 unit board: Mask(0x8 3)
    Router port(s):total 1 port.
            GE2/0/1                (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
```

```
    (1.1.1.1, 224.1.1.1):
      Attribute:    Host Port
      Host port unit board: Mask(0x8 3)
      Host port(s):total 1 port.
        GE2/0/2                (D)
MAC group(s):
  MAC group address:0100-5e01-0101
      Host port unit board: Mask(0x8 3)
      Host port(s):total 1 port.
        GE2/0/2
```

Table 1-2 display igmp group port-info command output description

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of IP 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 a dynamic port, S for a static port, and C for a port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for a real egress sub-VLAN under the current entry, and C for a 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 dynamic member port or router port aging timer. To get this time value of a non-aggregation port on a board other than the SRPU, you must specify the number of the slot where the corresponding board resides by using **slot** *slot-number*. This is not required for an aggregation port.
IP group address	Address of the IP multicast group
MAC group address	Address of the MAC multicast group
Attribute	Attribute of the IP multicast group
Host port(s)	Number of member ports

display igmp interface

Syntax

display igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

interface-type interface-number: Specifies an interface to display the IGMP configuration and operation information about. If no interface is specified, this command will display the related information of all IGMP-enabled interfaces.

verbose: Displays the detailed IGMP configuration and operation information.

Description

Use the **display igmp interface** command to view IGMP configuration and operation information of the specified interface or all IGMP-enabled interfaces.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the IGMP configuration and operation information on VLAN-interface 1 in the public instance.

```
<Sysname> display igmp interface Vlan-interface 1 verbose
     Vlan-interface1(10.10.1.20):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Value of last member query interval(in seconds): 1
   Value of startup query interval(in seconds): 15
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:54
   Querier for IGMP: 10.10.1.20 (this router)
   IGMP activity: 1 joins, 0 leaves
   Multicast routing on this interface: enabled
   Robustness: 2
   Require-router-alert: disabled
   Fast-leave: disabled
   Ssm-mapping: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
  Total 1 IGMP Group reported
```

Table 1-3 display igmp interface command output description

Field	Description
Vlan-interface1(10.10.1.20)	Interface name (IP address)
Current IGMP version	Version of IGMP currently running on the interface
Value of query interval for IGMP(in seconds)	IGMP query interval, in seconds

Field	Description
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Value of last member query interval(in seconds)	IGMP last member query interval, in seconds
Value of startup query interval(in seconds)	IGMP startup query interval, in seconds
Value of startup query count	Number of IGMP general queries the device sends on startup
General query timer expiry	Remaining time of the IGMP general query timer, where “off” means that the timer never expires
Querier for IGMP	IP address of the IGMP querier
IGMP activity	Statistics of IGMP activities (joins and leaves)
Robustness	Robustness variable of the IGMP querier
Require-router-alert	Dropping IGMP messages without Router-Alert (enabled/disabled)
Fast-leave	Fast leave processing status (enabled/disabled)
Ssm-mapping	IGMP SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of the startup query timer, where “off” means that the timer never expires
Other-querier-present-timer-expiry	Remaining time of the other querier present timer, where “off” means that the timer never expires
Total 1 IGMP Group reported	Total number of reported groups on the interface

display igmp routing-table

Syntax

display igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }]] *

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast source address, this argument has an effective value range of 0 to 32; for a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

Description

Use the **display igmp routing-table** command to view the IGMP routing table information.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View IGMP routing table information in the public instance.

```
<Sysname> display igmp routing-table
Routing table of VPN-Instance: public net
 Total 2 entries

 00001. (*, 225.1.1.1)
       List of 1 downstream interface
        Vlan-interface1 (20.1.1.1),
                   Protocol: STATIC

 00002. (*, 239.255.255.250)
       List of 1 downstream interface
        Vlan-interface2 (40.20.20.20),
                   Protocol: IGMP
```

Table 1-4 display igmp routing-table command output description

Field	Description
Routing table of VPN-Instance: public net	Public network IGMP routing table
00001	Sequence number of this (*, G) entry
(*, 225.1.1.1)	A (*, G) entry of the IGMP routing table
List of 1 downstream interface	Downstream interface list, namely the interfaces to which multicast data for this group will be forwarded
Protocol	Protocol type

display igmp ssm-mapping

Syntax

display igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **ssm-mapping** *group-address*

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255.

Description

Use the **display igmp ssm-mapping** command to view the configured IGMP SSM mappings for the specified multicast group.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Related commands: **ssm-mapping**.

Examples

View the IGMP SSM mappings for multicast group 232.1.1.1 in the public instance.

```
<Sysname> display igmp ssm-mapping 232.1.1.1
 VPN-Instance: public net
 Group: 232.1.1.1
 Source list:
        1.2.3.4
        5.5.5.5
        10.1.1.1
        100.1.1.10
```

Table 1-5 display igmp ssm-mapping command output description

Field	Description
VPN-Instance: public net	Public instance
Group	Multicast group address
Source list	List of multicast source addresses

display igmp ssm-mapping group

Syntax

display igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **ssm-mapping group** [*group-address* | **interface** *interface-type interface-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255.

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

verbose: Displays the detailed multicast group information created based on the configured IGMP SSM mappings.

Description

Use the **display igmp ssm-mapping group** command to view the multicast group information created based on the configured IGMP SSM mappings.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.
- If you do not specify a multicast group, this command will display the information of all multicast groups created based on the configured IGMP SSM mappings.
- If you do not specify an interface, this command will display the multicast group information created based on the configured IGMP SSM mappings on all the interfaces.

Examples

View the detailed information of multicast group 232.1.1.1 created based on the configured IGMP SSM mappings in the public instance.

```
<Sysname> display igmp ssm-mapping group 232.1.1.1 verbose
Interface group report information of VPN-Instance: public net
 Vlan-interface1 (10.10.10.10):
  Total 1 IGMP SSM-mapping Group reported
   Group: 232.1.1.1
     Uptime: 00:00:31
     Expires: off
     Last reporter: 1.1.1.1
     Version1-host-present-timer-expiry: off
     Source list(Total 1 source):
       Source: 1.1.1.1
          Uptime: 00:00:31
          Expires: 00:01:39
          Last-member-query-counter: 0
          Last-member-query-timer-expiry: off
```

Table 1-6 display igmp ssm-mapping group command output description

Field	Description
Interface group report information of VPN-Instance: public net	Multicast group information created based on IGMP SSM mappings on a public network interface
Total 1 IGMP SSM-mapping Group reported	One IGMP SSM mapping multicast group was reported.
Group	Multicast group address
Uptime	Length of time since the multicast group was reported
Expires	Remaining time of the multicast group, where “off” means that the multicast group never times out
Last reporter	Address of the last host that reported its membership for this multicast group
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where “off” means that the timer never expires
Source list(Total 1 source)	Multicast source list (one multicast source)
Source	Multicast source address
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer, where “off” means that the timer never expires

igmp

Syntax

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

Description

Use the **igmp** command to enter public instance IGMP view or VPN instance IGMP view .

Use the **undo igmp** command to remove configurations performed in public instance IGMP view or VPN instance IGMP view.

Note that:

- If you do not specify **vpn-instance**, this configuration will take effect only on the public instance.
- IP multicast must be enabled in the corresponding instance before this command can take effect

Related commands: **igmp enable**; **multicast routing-enable** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IP multicast routing in the public instance and enter public instance IGMP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

Enable IP multicast routing in VPN instance mvpn and enter IGMP view for VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn]
```

igmp enable

Syntax

igmp enable

undo igmp enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **igmp enable** command to enable IGMP on the current interface.

Use the **undo igmp enable** command to disable IGMP on the current interface.

By default, IGMP is disabled on all interfaces.

Note that:

- IP multicast must be enabled in the corresponding instance before this command can take effect.
- IGMP must be enabled on an interface before any other IGMP feature configured on the interface can take effect.

Related commands: **igmp**; **multicast routing-table** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IP multicast routing, and then enable IGMP on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

igmp group-policy

Syntax

igmp group-policy *acl-number* [*version-number*]

undo igmp group-policy

View

Interface 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..

version-number: IGMP version, in the range of 1 to 3. If you do not specify an IGMP version, the configured group filter will apply to IGMP reports of all versions.

Description

Use the **igmp group-policy** command to configure a multicast group filter on the current interface to control joins to specific multicast groups.

Use the **undo igmp group-policy** command to remove the configured multicast group filter.

By default, no multicast group filter is configured, namely a host can join any valid multicast group.

Examples

Configure an ACL rule so that hosts on the subnet attached to VLAN-interface 1 can join multicast group 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] igmp group-policy 2005
```

igmp last-member-query-interval

Syntax

igmp last-member-query-interval *interval*

undo igmp last-member-query-interval

View

Interface view

Default Level

2: System level

Parameters

interval: IGMP last member query interval in seconds, with an effective range of 1 to 5.

Description

Use the **igmp last-member-query-interval** command to configure the last member query interval, namely the length of time the device waits between sending IGMP group-specific queries, on the current interface.

Use the **undo igmp last-member-query-interval** command to restore the system default.

By default, the IGMP last member query interval is 1 second.

Related commands: **last-member-query-interval**, **igmp robust-count**, **display igmp interface**.

Examples

Set the IGMP last member query interval to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp last-member-query-interval 3
```

igmp max-response-time

Syntax

igmp max-response-time *interval*

undo igmp max-response-time

View

Interface view

Default Level

2: System level

Parameters

interval: Maximum response time in seconds for IGMP general queries, with an effective range of 1 to 25.

Description

Use the **igmp max-response-time** command to configure the maximum response time for IGMP general queries on the current interface.

Use the **undo igmp max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **max-response-time**, **igmp timer other-querier-present**, **display igmp interface**.

Examples

Set the maximum response time for IGMP general queries to 8 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp max-response-time 8
```

igmp require-router-alert

Syntax

igmp require-router-alert

undo igmp require-router-alert

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **igmp require-router-alert** command to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo igmp require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it passes all the IGMP messages it receives to the upper layer protocol for processing.

Related commands: **require-router-alert**, **igmp send-router-alert**.

Examples

Configure VLAN-interface 100 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp require-router-alert
```

igmp robust-count

Syntax

igmp robust-count *robust-value*

undo igmp robust-count

View

Interface view

Default Level

2: System level

Parameters

robust-value: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the default number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

Description

Use the **igmp robust-count** command to configure the IGMP querier robustness variable on the current interface.

Use the **undo igmp robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related commands: **robust-count**, **igmp timer query**, **igmp last-member-query-interval**, **igmp timer other-querier-present**, **display igmp interface**.

Examples

Set the IGMP querier robustness variable to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp robust-count 3
```

igmp send-router-alert

Syntax

igmp send-router-alert

undo igmp send-router-alert

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **igmp send-router-alert** command on the current interface to enable insertion of the Router-Alert option in IGMP messages to be sent.

Use the **undo igmp send-router-alert** command on the current interface to disable insertion of the Router-Alert option in IGMP messages to be sent.

By default, IGMP messages are sent with the Router-Alert option.

Related commands: **send-router-alert**, **igmp require-router-alert**.

Examples

Disable insertion of the Router-Alert option into IGMP messages that leave VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo igmp send-router-alert
```

igmp ssm-mapping enable

Syntax

igmp ssm-mapping enable

undo igmp ssm-mapping enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **igmp ssm-mapping enable** command to enable the IGMP SSM mapping feature on the current interface.

Use the **undo igmp ssm-mapping enable** command to disable the IGMP SSM mapping feature on the current interface.

By default, the IGMP SSM mapping feature is disabled on all interfaces.

Examples

Enable the IGMP SSM mapping feature on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp ssm-mapping enable
```

igmp startup-query-count

Syntax

igmp startup-query-count *value*

undo igmp startup-query-count

View

Interface view

Default Level

2: System level

Parameters

value: Startup query count, namely, the number of queries the IGMP querier sends on startup, with an effective range of 2 to 5.

Description

Use the **igmp startup-query-count** command to configure the startup query count on the current interface.

Use the **undo igmp startup-query-count** command to restore the system default.

By default, the startup query count is set to the IGMP querier robustness variable.

 **Note**

By default, the IGMP querier robustness variable is 2, so the startup query count is also 2.

Related commands: **startup-query-count**, **igmp robust-count**.

Examples

Set the startup query count to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-count 3
```

igmp startup-query-interval

Syntax

igmp startup-query-interval *interval*

undo igmp startup-query-interval

View

Interface view

Default Level

2: System level

Parameters

interval: Startup query interval in seconds, namely, the interval between general queries the IGMP querier sends on startup, with an effective range of 1 to 18000.

Description

Use the **igmp startup-query-interval** command to configure the startup query interval on the current interface.

Use the **undo igmp startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the IGMP query interval.

Note

By default, the IGMP query interval is 60 seconds, so the startup query interval = 60 / 4 = 15 (seconds).

Related commands: **startup-query-interval**, **igmp timer query**.

Examples

Set the startup query interval to 5 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-interval 5
```

igmp static-group

Syntax

igmp static-group *group-address* [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**source** *source-address*] }

View

Interface view

Default Level

2: System level

Parameters

all: Specifies to remove all static multicast groups that the current interface has joined.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address.

Description

Use the **igmp static-group** command to configure the current interface to be a statically connected member of the specified multicast group or multicast source and group.

Use the **undo igmp static-group** command to restore the system default.

By default, an interface is not a static member of any multicast group or multicast source and group.

If the specified multicast address is in the SSM multicast address range, you must specify a multicast source address at the same time; otherwise IGMP routing table entries cannot be established. There is no such a restriction if the specified multicast group address is not in the SSM multicast address range.

Examples

Configure VLAN-interface 1 to be a statically connected member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] igmp static-group 224.1.1.1
```

Configure VLAN-interface 1 to be a statically connected member of multicast source and group (192.168.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp timer other-querier-present

Syntax

igmp timer other-querier-present *interval*

undo igmp timer other-querier-present

View

Interface view

Default Level

2: System level

Parameters

interval: IGMP other querier present interval in seconds, in the range of 60 to 300.

Description

Use the **igmp timer other-querier-present** command to configure the IGMP other querier present interval on the current interface.

Use the **undo igmp timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [IGMP query interval] times [IGMP querier robustness variable] plus [maximum response time for IGMP general queries] divided by two.

Note

By default, the three parameters in the above-mentioned formula are 60 (seconds), 2 and 10 (seconds) respectively, so the IGMP other querier present interval = 60 × 2 + 10 / 2 = 125 (seconds).

Related commands: **timer other-querier-present**, **igmp timer query**, **igmp robust-count**, **igmp max-response-time**, **display igmp interface**.

Examples

Set the IGMP other querier present interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer other-querier-present 200
```

igmp timer query

Syntax

igmp timer query *interval*

undo igmp timer query

View

Interface view

Default Level

2: System level

Parameters

interval: IGMP query interval in seconds, namely the interval between IGMP general queries, with an effective range of 1 to 18,000.

Description

Use the **igmp timer query** command to configure the IGMP query interval on the current interface.

Use the **undo igmp timer query** command to restore the system default.

By default, the IGMP query interval is 60 seconds.

Related commands: **timer query**, **igmp timer other-querier-present**, **display igmp interface**.

Examples

Set the IGMP query interval to 125 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer query 125
```

igmp version

Syntax

igmp version *version-number*

undo igmp version

View

Interface view

Default Level

2: System level

Parameters

version-number: IGMP version, in the range of 1 to 3.

Description

Use the **igmp version** command to configure the IGMP version on the current interface.

Use the **undo igmp version** command to restore the default IGMP version.

The default IGMP version is version 2.

Related commands: **version**.

Examples

Set the IGMP version to IGMPv1 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp version 1
```

last-member-query-interval (IGMP view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

interval: Last-member query interval in seconds, with an effective range of 1 to 5.

Description

Use the **last-member-query-interval** command to configure the global IGMP last-member query interval.

Use the **undo last-member-query-interval** command to restore the system default.

By default, the IGMP last-member query interval is 1 second.

Related commands: **igmp last-member-query-interval**, **robust-count**, **display igmp interface**.

Examples

Set the global IGMP last-member interval to 3 seconds in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 3
```

max-response-time (IGMP view)

Syntax

max-response-time *interval*

undo max-response-time

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

interval: Maximum response time for IGMP general queries in seconds, with an effective range of 1 to 25.

Description

Use the **max-response-time** command to configure the maximum response time for IGMP general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **igmp max-response-time**, **timer other-querier-present**, **display igmp interface**.

Examples

Set the maximum response time for IGMP general queries to 8 seconds globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 8
```

require-router-alert (IGMP view)

Syntax

require-router-alert

undo require-router-alert

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

None

Description

Use the **require-router-alert** command to configure globally the router to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo require-router-alert** command to restore the system default.

By default, the device does not check the Router-Alert option, namely it handles all the IGMP messages it received to the upper layer protocol for processing.

Related commands: **igmp require-router-alert**, **send-router-alert**.

Examples

Globally configure the router to discard IGMP messages that do not carry the Router-Alert option in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

reset igmp group

Syntax

reset igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space

all: The first **all** specifies to clear IGMP multicast group information on all interfaces, while the second **all** specifies to clear the information of all IGMP multicast groups.

interface *interface-type interface-number*: Clears IGMP multicast information on the specified interface.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Multicast source address.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

Description

Use the **reset igmp group** command to clear IGMP multicast group information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance
- This command cannot clear IGMP multicast group information of static joins.

Related commands: **display igmp group**.

Examples

Clear all IGMP multicast group information on all interfaces.

```
<Sysname> reset igmp group all
```

Clear all IGMP multicast group information on VLAN-interface 100.

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

Clear IGMP multicast group information about multicast group 225.0.0.1 on VLAN-interface 100.

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

reset igmp group port-info

Syntax

reset igmp group port-info { **all** | *group-address* } [**vlan** *vlan-id*]

View

User view

Default Level

2: System level

Parameters

all: Clears Layer 2 port information of all the IGMP multicast groups.

group-address: Clears Layer 2 port information of the specified IGMP multicast group. The effective range of *group-address* is 224.0.1.0 to 239.255.255.255.

vlan-id: Clears Layer 2 port information of IGMP multicast groups in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

Description

Use the **reset igmp group port-info** command to clear Layer 2 port information of IGMP multicast groups.

Note that:

- Layer 2 ports for IGMP multicast groups include member ports and router ports.
- This command cannot clear Layer 2 port information about IGMP multicast groups of static joins.

Related commands: **display igmp group port-info**.

Examples

Clear Layer 2 port information of all IGMP multicast groups in all VLANs.

```
<Sysname> reset igmp group port-info all
```

Clear Layer 2 port information of all IGMP multicast groups in VLAN 100.

```
<Sysname> reset igmp group port-info all vlan 100
```

Clear Layer 2 port information about multicast group 225.0.0.1 in VLAN 100.

```
<Sysname> reset igmp group port-info 225.0.0.1 vlan 100
```

reset igmp ssm-mapping group

Syntax

reset igmp [**all-instance** | **vpn-instance** *vpn-instance-name*] **ssm-mapping group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

all: The first **all** specifies to clear multicast group information created based on the configured IGMP SSM mappings on all interfaces, while the second **all** specifies to clear all multicast group information created based on the configured IGMP SSM mappings.

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

group-address: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source by its IP address.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. For both cases, the default value is 32.

Description

Use the **reset igmp ssm-mapping group** command to clear multicast group information created based on the configured IGMP SSM mappings.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will clear the information on the public instance.

Related commands: **display igmp ssm-mapping group**.

Examples

Clear all multicast group information created based on the configured IGMP SSM mappings on all interfaces in the public instance.

```
<Sysname> reset igmp ssm-mapping group all
```

robust-count (IGMP view)

Syntax

robust-count *robust-value*

undo robust-count

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

robust-value: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the default number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

Description

Use the **robust-count** command to configure the IGMP querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related commands: **igmp robust-count**, **timer query**, **last-member-query-interval**, **timer other-querier-present**, **display igmp interface**.

Examples

Set the IGMP querier robustness variable to 3 globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 3
```

send-router-alert (IGMP view)

Syntax

send-router-alert

undo send-router-alert

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

None

Description

Use the **send-router-alert** command to globally enable insertion of the Router-Alert option into IGMP messages to be sent.

Use the **undo send-router-alert** command to globally disable insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

Related commands: **igmp send-router-alert**, **require-router-alert**.

Examples

Globally disable the insertion of the Router-Alert option in IGMP messages to be sent in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] undo send-router-alert
```

ssm-mapping (IGMP view)

Syntax

ssm-mapping *group-address* { *mask* | *mask-length* } *source-address*

undo ssm-mapping { *group-address* { *mask* | *mask-length* } *source-address* | **all** }

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

group-address: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Subnet mask of the multicast group address.

mask-length: Subnet mask length of the multicast group address, in the range of 4 to 32.

source-address: Specifies a multicast source by its IP address.

all: Removes all IGMP SSM mappings.

Description

Use the **ssm-mapping** command to configure an IGMP SSM mapping.

Use the **undo ssm-mapping** command to remove one or all IGMP SSM mappings.

By default, no IGMP SSM mappings are configured.

Related commands: **igmp ssm-mapping enable**, **display igmp ssm-mapping**.

Examples

Configure an IGMP SSM mapping in the public instance for multicast groups in the range of 225.1.1.0/24 and multicast source 125.1.1.1.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] ssm-mapping 225.1.1.0 24 125.1.1.1
```

startup-query-count (IGMP view)

Syntax

startup-query-count *value*

undo startup-query-count

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

value: Startup query count, namely, the number of queries the IGMP querier sends on startup, with an effective range of 2 to 5.

Description

Use the **startup-query-count** command to configure the startup query count globally.

Use the **undo startup-query-count** command to restore the system default.

By default, the startup query count is set to the IGMP querier robustness variable.

Note

By default, the IGMP querier robustness variable is 2, so the startup query count is also 2.

Related commands: **igmp startup-query-count**, **robust-count**.

Examples

Set the startup query count to 3 globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-count 3
```

startup-query-interval (IGMP view)

Syntax

startup-query-interval *interval*

undo startup-query-interval

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

interval: Startup query interval in seconds, namely, the interval between general queries the IGMP querier sends on startup, with an effective range of 1 to 18000.

Description

Use the **startup-query-interval** command to configure the startup query interval globally.

Use the **undo startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the “IGMP query interval”.

Note

By default, the IGMP query interval is 60 seconds, so the startup query interval = 60 / 4 = 15 (seconds).

Related commands: **igmp-startup-query-interval**, **timer query**.

Examples

Set the startup query interval to 5 seconds globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-interval 5
```

timer other-querier-present (IGMP view)

Syntax

timer other-querier-present *interval*

undo timer other-querier-present

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

interval: IGMP other querier present interval, in the range of 60 to 300.

Description

Use the **timer other-querier-present** command to configure the IGMP other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [IGMP query interval] times [IGMP querier robustness variable] plus [maximum response time for IGMP general queries] divided by two.

Note

By default, the three parameters in the above-mentioned formula are 60 (seconds), 2 (times) and 10 (seconds) respectively, so the IGMP other querier present interval = 60 × 2 + 10 / 2 = 125 (seconds).

Related commands: **igmp timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display igmp interface**.

Examples

Set the IGMP other querier present interval to 200 seconds globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

timer query (IGMP view)

Syntax

timer query *interval*

undo timer query

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

interval: IGMP query interval in seconds, namely interval between IGMP general queries, with an effective range of 1 to 18,000.

Description

Use the **timer query** command to configure the IGMP query interval globally.

Use the **undo timer query** command to restore the default setting.

By default, IGMP query interval is 60 seconds.

Related commands: **igmp timer query**, **timer other-querier-present**, **display igmp interface**.

Examples

Set the IGMP query interval to 125 seconds globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer query 125
```

version (IGMP view)

Syntax

version *version-number*

undo version

View

Public instance IGMP view, VPN instance IGMP view

Default Level

2: System level

Parameters

version-number: IGMP version, in the range of 1 to 3.

Description

Use the **version** command to configure the IGMP version globally.

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

The default IGMP version is version 2.

Related commands: **igmp version**.

Examples

Set the global IGMP version to IGMPv1 in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] version 1
```

Table of Contents

1 PIM Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running the PIM protocol.

PIM Configuration Commands

auto-rp enable

Syntax

auto-rp enable

undo auto-rp enable

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

None

Description

Use the **auto-rp enable** command to enable auto-RP.

Use the **undo auto-rp enable** command to disable auto-RP.

By default, auto-RP is disabled.

Related commands: **static-rp**.

Examples

Enable auto-RP in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

bsr-policy (PIM view)

Syntax

bsr-policy *acl-number*

undo bsr-policy

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

Description

Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely the bootstrap messages from any source are regarded to be valid.

Examples

Configure a legal BSR address range in the public instance so that only routers on the segment 10.1.1.0/24 can become the BSR.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2000
```

c-bsr (PIM view)

Syntax

c-bsr *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number. This configuration can take effect only if PIM-SM is enabled on the interface.

hash-length: Hash mask length, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description

Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Note that PIM-SM must be enabled on the interface to be configured as a C-BSR.

Related commands: **pim sm**, **c-bsr hash-length**, **c-bsr priority**, **c-rp**.

Examples

Configure VLAN-interface 100 to be a C-BSR.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr vlan-interface 100
```

c-bsr admin-scope

Syntax

c-bsr admin-scope

undo c-bsr admin-scope

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

None

Description

Use the **c-bsr admin-scope** command to enable administrative scoping.

Use the **undo c-bsr admin-scope** command to disable administrative scoping.

By default, BSR administrative scoping is disabled, namely there is only one BSR in a PIM-SM domain.

Related commands: **c-bsr**, **c-bsr group**, **c-bsr global**.

Examples

Enable administrative scoping in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr admin-scope
```

c-bsr global

Syntax

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

hash-length: Hash mask length in the global scope zone, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the global scope zone, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description

Use the **c-bsr global** command to configure a C-BSR for the global scope zone.

Use the **undo c-bsr global** command to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

Related commands: **c-bsr group**, **c-bsr hash-length**, **c-bsr priority**.

Examples

Configure the router to be a C-BSR for the global scope zone in the public instance, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr global priority 1
```

c-bsr group

Syntax

c-bsr group *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

group-address: Multicast group address, in the range of 239.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address, in the range of 8 to 32.

hash-length: Hash mask length in the admin-scope region corresponding to the specified multicast group, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the admin-scope region corresponding to a multicast group, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description

Use the **c-bsr group** command to configure a C-BSR for the admin-scope region associated with the specified group.

Use the **undo c-bsr group** command to remove the C-BSR configuration for the admin-scope region associated with the specified group.

By default, no C-BSRs are configured for admin-scope regions.

Related commands: **c-bsr global**, **c-bsr admin-scope**, **c-bsr hash-length**, **c-bsr priority**.

Examples

In the public instance configure the router to be a C-BSR in the admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

c-bsr hash-length (PIM view)

Syntax

c-bsr hash-length *hash-length*

undo c-bsr hash-length

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

hash-length: Hash mask length, in the range of 0 to 32.

Description

Use the **c-bsr hash-length** command to configure the global Hash mask length .

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length is 30.

Related commands: **c-bsr**, **c-bsr global**, **c-bsr group**.

Examples

Set the global Hash mask length to 16 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

c-bsr holdtime (PIM view)

Syntax

c-bsr holdtime *interval*

undo c-bsr holdtime

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: BS timeout in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **c-bsr holdtime** command to configure the BS timeout, namely the length of time a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the bootstrap timeout value is determined by this formula: BS timeout = BS period × 2 + 10.

 **Note**

The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr**, **c-bsr interval**.

Examples

Set the BS timeout time to 150 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr holdtime 150
```

c-bsr interval (PIM view)

Syntax

c-bsr interval *interval*

undo c-bsr interval

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: BS period in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **c-bsr interval** command to configure the BS period, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the system default.

By default, the BS period value is determined by this formula: BS period = (BS timeout – 10) ÷ 2.

Note

The default BS timeout is 130 seconds, so the default BS period = (130 – 10) ÷ 2 = 60 (seconds).

Related commands: **c-bsr**, **c-bsr holdtime**.

Examples

Set the BS period to 30 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr interval 30
```

c-bsr priority (PIM view)

Syntax

c-bsr priority *priority*

undo c-bsr priority

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

priority: Priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority.

Description

Use the **c-bsr priority** command to configure the global C-BSR priority.

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

By default, the C-BSR priority is 0.

Related commands: **c-bsr**, **c-bsr global**, **c-bsr group**.

Examples

Set the global C-BSR priority to 5 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5
```

c-rp (PIM view)

Syntax

c-rp *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interface-type interface-number: Specifies an interface, the IP address of which will be advertised as a C-RP address.

acl-number: Basic ACL number, in the range of 2000 to 2999. This ACL defines a range of multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any group range matching the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value of this argument means a lower priority.

hold-interval: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

Description

Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- PIM-SM must be enabled on the interface to be configured as a C-RP.
- If you do not specify a group range for the C-RP, the C-RP will serve all multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these multiple group ranges in multiple rules in the ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

Examples

Configure VLAN-interface 100 to be a C-RP for multicast groups 225.1.0.0/16 and 226.2.0.0/16, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp vlan-interface 100 group-policy 2000 priority 10
```

c-rp advertisement-interval (PIM view)

Syntax

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description

Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples

Set the global C-RP-Adv interval to 30 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30
```

c-rp holdtime (PIM view)

Syntax

c-rp holdtime *interval*

undo c-rp holdtime

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description

Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of C-RP information in BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-rp**, **c-bsr interval**.

Examples

Set the global C-RP timeout time to 200 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp holdtime 200
```

crp-policy (PIM view)

Syntax

crp-policy *acl-number*

undo crp-policy

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

acl-number: Advanced ACL number, in the range of 3000 to 3999. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP and the **destination** keyword specifies the address range of the multicast groups that the C-RP will serve.

Description

Use the **crp-policy** command to configure a legal C-RP address range and the range of served multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are accepted.

Note that the **crp-policy** command filters the multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the multicast group range advertised by a C-RP is 224.1.0.0/16 while the legal group range defined by the **crp-policy** command is 224.1.0.0/30, the multicast groups in the range of 224.1.0.0/16 are allowed to pass.

Related commands: **c-rp**.

Examples

In the public instance, configure a C-RP address range so that only routers in the address range of 1.1.1.1/24 can be C-RPs

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0 0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

display pim bsr-info

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **bsr-info**

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

Description

Use the **display pim bsr-info** command to view the BSR information in the PIM domain and the locally configured C-RP information in effect.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Related commands: **c-bsr**, **c-rp**.

Examples

View the BSR information in the PIM-SM domain in the public instance and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
 VPN-Instance: public net
 Elected BSR Address: 12.12.12.9
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Global
     Uptime: 00:00:56
     Next BSR message scheduled at: 00:01:14
 Candidate BSR Address: 12.12.12.9
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Global

 Candidate RP: 12.12.12.9(LoopBack1)
     Priority: 0
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
 Candidate RP: 3.3.3.3(Vlan-interface1)
     Priority: 20
     HoldTime: 90
     Advertisement Interval: 50
     Next advertisement scheduled at: 00:00:28
```

```
Candidate RP: 5.5.5.5(Vlan-interface2)
    Priority: 0
    HoldTime: 80
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
```

Table 1-1 display pim bsr-info command output description

Field	Description
VPN-Instance: public net	Public instance
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up, in hh:mm:ss
Next BSR message scheduled at	Length of time in which the BSR will expire, in hh:mm:ss
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message, in hh:mm:ss

display pim claimed-route

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

source-address: Displays the information of the unicast route to a particular multicast source. If you do not provide this argument, this command will display the information about all unicast routes used by PIM.

Description

Use the **display pim claimed-route** command to view the information of unicast routes used by PIM.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.
- If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

Examples

View the information of all unicast routes used by PIM in the public instance.

```
<Sysname> display pim claimed-route
 VPN-Instance: public net
 RPF information about: 172.168.0.0
     RPF interface: Vlan-interface1, RPF neighbor: 172.168.0.2
     Referenced route/mask: 172.168.0.0/24
     Referenced route type: unicast (direct)
     RPF-route selecting rule: preference-preferred
     The (S,G) or (*,G) list dependent on this route entry
     (172.168.0.12, 227.0.0.1)
```

Table 1-2 display pim claimed-route command output description

Field	Description
VPN-Instance: public net	Public instance
RPF information about: 172.168.0.0	Information of the route to the multicast source 172.168.0.0
RPF interface	RPF interface type and number
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Address/mask of the referenced route
Referenced route type	Type of the referenced route: • igp: IGP unicast route • egp: EGP unicast route • unicast (direct): Direct unicast route • unicast: Other unicast route (such as static unicast route) • mbgp: MBGP route • multicast static: Static multicast route
RPF-route selecting rule	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entry list dependent on this RPF route

display pim control-message counters

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

probe: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of Bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of Graft messages.

graft-ack: Displays the number of Graft-ack messages.

hello: Displays the number of Hello messages.

join-prune: Displays the number of Join/prune messages.

state-refresh: Displays the number of state refresh messages.

Description

Use the **display pim control-message counters** command to view the statistics information of PIM control messages.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the statistics information of all types of PIM control messages on all interfaces in the public instance.

```
<Sysname> display pim control-message counters
 VPN-Instance: public net
 PIM global control-message counters:
                  Received         Sent             Invalid
```

```
Register          20                37                2
Register-Stop     25                20                1
Probe             10                5                 0

PIM control-message counters for interface: Vlan-interface1
                  Received          Sent              Invalid
Assert            10                5                 0
Graft             20                37                2
Graft-Ack         25                20                1
Hello             1232              453               0
Join/Prune        15                30                21
State-Refresh     8                 7                 1
BSR               3243              589               1
C-RP              53                32                0
```

Table 1-3 display pim control-message counters command output description

Field	Description
VPN-Instance: public net	Public instance
PIM global control-message counters	Statistics of PIM global control messages
PIM control-message counters for interface	Interface for which PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

display pim grafts

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **grafts**

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

Description

Use the **display pim grafts** command to view the information about unacknowledged graft messages.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the information about unacknowledged graft messages in the public instance.

```
<Sysname> display pim grafts
 VPN-Instance: public net
 Source             Group            Age          RetransmitIn
 192.168.10.1       224.1.1.1        00:00:24     00:00:02
```

Table 1-4 display pim grafts command output description

Field	Description
VPN-Instance: public net	Public instance
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hh:mm:ss
RetransmitIn	Time in which the graft message will be retransmitted, in hh:mm:ss

display pim interface

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

interface-type interface-number: Displays the PIM information on a particular interface.

verbose: Displays the detailed PIM information.

Description

Use the **display pim interface** command to view the PIM information on the specified interface or all interfaces.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the PIM information on all interfaces in the public instance.

```
<Sysname> display pim interface
 VPN-Instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan1               1      30         1          10.1.1.2
 Vlan2               0      30         1          172.168.0.2    (local)
 Vlan3               1      30         1          20.1.1.2
```

Table 1-5 display pim interface command output description

Field	Description
VPN-Instance: public net	Public instance
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address

View the detailed PIM information on Vlan-interface 1 in the public instance.

```
<Sysname> display pim interface vlan-interface 1 verbose
 VPN-Instance: public net
 Interface: Vlan-interface1, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
```

```
PIM override interval (configured): 2500 ms
PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
PIM generation ID: 0xF5712241
PIM require generation ID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2
```

Table 1-6 display pim interface verbose command output description

Field	Description
VPN-Instance: public net	Public instance
Interface	Interface name and its IP address
PIM version	Running PIM version
PIM mode	PIM mode, dense or sparse
PIM DR	DR IP address
PIM DR Priority (configured)	Configured priority for DR election
PIM neighbor count	Total number of PIM neighbors
PIM hello interval	Hello interval
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time

Field	Description
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim join-prune

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] * [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

mode: Displays the information of join/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

flags *flag-value*: Displays routing entries containing the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

neighbor-address: Displays the information of join/prune messages to send to the specified PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

Description

Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

In the public instance view the information of join/prune messages to send in the PIM-SM mode.

```
<Sysname> display pim join-prune mode sm
 VPN-Instance: public net

 Expiry Time: 50 sec
 Upstream nbr: 10.1.1.1 (Vlan-interface1)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
 ------------------------------------------------------------------------
 Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 1-7 display pim join-prune command output description

Field	Description
VPN-Instance: public net	Public instance
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IP address of the upstream PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim neighbor

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **neighbor** [**interface** *interface-type interface-number* | *neighbor-address* | **verbose**] *

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

interface-type interface-number: Displays the PIM neighbor information on a particular interface.

neighbor-address: Displays the information of a particular PIM neighbor.

verbose: Displays the detailed PIM neighbor information.

Description

Use the **display pim neighbor** command to view the PIM neighbor information.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the information of all PIM neighbors in the public instance.

```
<Sysname> display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 10.1.1.2        Vlan1               02:50:49 00:01:31 1
 20.1.1.2        Vlan2               02:49:39 00:01:42 1
```

In the public instance, view the detailed information of the PIM neighbor whose IP address is 11.110.0.20.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
 VPN-Instance: public net
 Neighbor: 11.110.0.20
     Interface: Vlan-interface3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
     Generation ID: 0x2ACEFE15
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     State refresh interval: 60 s
     Neighbor tracking: Disabled
```

Table 1-8 display pim neighbor command output description

Field	Description
VPN-Instance: public net	Public instance
Total Number of Neighbors	Total number of PIM neighbors
Neighbor	IP address of the PIM neighbor
Interface	Interface connecting the PIM neighbor
Uptime	Length of time for which the PIM neighbor has been up, in hh:mm:ss
Expires/Expiry time	Remaining time of the PIM neighbor, in hh:mm:ss; “never” means that the PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the PIM neighbor
Generation ID	Generation ID of the PIM neighbor (a random value indicating a status change of the PIM neighbor)
Holdtime	Holdtime of the PIM neighbor; “forever” means that the PIM neighbor is always up and reachable

Field	Description
LAN delay	Prune delay
Override interval	Prune override interval
State refresh interval	Interval of sending state refresh messages
Neighbor tracking	Neighbor tracking status (enabled/disabled)

display pim routing-table

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Multicast source address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address, in the range of 0 to 32. The system default is 32.

incoming-interface: Displays PIM routing entries that contain the specified interface as the incoming interface.

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

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays PIM routing entries of which the outgoing interface is the specified interface.

include: Displays PIM routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays PIM routing entries of which the outgoing interface list excludes the specified interface.

match: Displays PIM routing entries of which the outgoing interface list includes only the specified interface.

mode *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

flags *flag-value*: Displays routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies PIM routing entries to which actual data has arrived.
- **del**: Specifies PIM routing entries scheduled to be deleted.
- **exprune**: Specifies PIM routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries containing outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on routers directly connecting to the same subnet with the multicast source.
- **msdp**: Specifies PIM routing entries learned from MSDP SA messages.
- **niif**: Specifies PIM routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor searching failure.
- **rpt**: Specifies PIM routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies PIM routing entries of the receiving side of the switch-MDT.
- **spt**: Specifies PIM routing entries on the SPT.
- **sq**: Specifies PIM routing entries of the originator side of switch-MDT switchover.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description

Use the **display pim routing-table** command to view PIM routing table information.

Related commands: **display multicast routing-table** in *Multicast Routing and Forwarding Commands* of the *IP Multicast Volume*.

Examples

View the content of the PIM routing table in the public instance.

```
<Sysname> display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlan-interface1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
```

```
1: Vlan-interface2
    Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 1-9 display pim routing-table command output description

Field	Description
VPN-Instance: public net	Public instance
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S,G) and (*, G) entries in the PIM routing table
(172.168.0.2, 227.0.0.1)	An (S, G) entry in the PIM routing table
Protocol	PIM mode, PIM-SM or PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the PIM routing table
Uptime	Length of time for which the (S, G) or (*, G) entry has been existing
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry • For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. • For a (S, G) entry, if this router directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	Information of the downstream interface(s), including: • Number of downstream interfaces • Downstream interface name • Protocol type on the downstream interface(s) • Uptime of the downstream interface(s) • Expiry time of the downstream interface(s)

display pim rp-info

Syntax

display pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Address of the multicast group of which the RP information is to be displayed, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide a group address, this command will display the RP information corresponding to all multicast groups.

Description

Use the **display pim rp-info** command to view the RP information.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.
- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Examples

View the RP information corresponding to the multicast group 224.0.1.1 in the public instance.

```
<Sysname> display pim rp-info 224.0.1.1
 VPN-Instance: public net
 BSR RP Address is: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:10
     Expires: 00:02:30
 RP mapping for this group is: 2.2.2.2
```

View the RP information corresponding to all multicast groups in the public instance.

```
<Sysname> display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:36
     Expires: 00:02:29
```

Table 1-10 display pim rp-info command output description

Field	Description
VPN-Instance: public net	Public instance
BSR RP Address is	IP address of the RP
Group/MaskLen	The multicast group served by the RP
RP	IP address of the RP
Priority	RP priority
HoldTime	RP timeout time
Uptime	Length of time for which the RP has been up, in hh:mm:ss

Field	Description
Expires	Length of time in which the RP will expire, in hh:mm:ss
RP mapping for this group	IP address of the RP serving the current multicast group

hello-option dr-priority (PIM view)

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description

Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: pim hello-option dr-priority.

Examples

Set the router priority for DR election to 3 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

hello-option holdtime (PIM view)

Syntax

hello-option holdtime *interval*

undo hello-option holdtime

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 means that the PIM neighbor is always reachable.

Description

Use the **hello-option holdtime** command to configure the PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **pim hello-option holdtime**.

Examples

Set the global value of the PIM neighbor timeout time to 120 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

hello-option lan-delay (PIM view)

Syntax

hello-option lan-delay *interval*

undo hello-option lan-delay

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option override-interval**, **pim hello-option override-interval**, **pim hello-option lan-delay**.

Examples

Set the LAN-delay time to 200 milliseconds globally in the public instance.

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

```
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

hello-option neighbor-tracking (PIM view)

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

None

Description

Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **pim hello-option neighbor-tracking**.

Examples

Disable join suppression globally in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
```

hello-option override-interval (PIM view)

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option lan-delay**, **pim hello-option lan-delay**, **pim hello-option override-interval**.

Examples

Set the prune override interval to 2,000 milliseconds globally in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

holdtime assert (PIM view)

Syntax

holdtime assert *interval*

undo holdtime assert

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, **pim holdtime assert**.

Examples

Set the global value of the assert timeout time to 100 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

holdtime join-prune (PIM view)

Syntax

holdtime join-prune *interval*

undo holdtime join-prune

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, **pim holdtime join-prune**.

Examples

Set the global value of the join/prune timeout time to 280 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

jp-pkt-size (PIM view)

Syntax

jp-pkt-size *packet-size*

undo jp-pkt-size

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

packet-size: Maximum size of join/prune messages in bytes, with an effective range of 100 to 8,100.

Description

Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

Examples

Set the maximum size of join/prune messages to 1,500 bytes in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

jp-queue-size (PIM view)

Syntax

jp-queue-size *queue-size*

undo jp-queue-size

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

queue-size: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

Description

Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune timeout time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size**, **holdtime join-prune**, **pim holdtime join-prune**.

Examples

Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

pim

Syntax

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

Description

Use the **pim** command to enter public instance PIM view or VPN instance PIM view.

Use the **undo pim** command to remove all configurations performed in public instance PIM view or VPN instance PIM view.

Note that:

- If **vpn-instance** is not specified, this configuration will take effect only on the public instance.
- IP multicast routing must be enabled in the corresponding instance before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands* of the *IP Multicast Volume*.

Examples

Enable IP multicast routing in the public instance and enter public instance PIM view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim]
```

Enable IP multicast routing in VPN instance mvpn and enter PIM view of VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

pim bsr-boundary

Syntax

pim bsr-boundary

undo pim bsr-boundary

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim bsr-boundary** command to configure a PIM domain border, namely a bootstrap message boundary.

Use the **undo pim bsr-boundary** command to remove the configured PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr**; **multicast boundary** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Configure VLAN-interface 100 as a PIM domain border.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim bsr-boundary
```

pim dm

Syntax

pim dm

undo pim dm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim dm** command to enable PIM-DM.

Use the **undo pim dm** command to disable PIM-DM.

By default, PIM-DM is disabled.

Note that:

- This command can take effect only after IP multicast routing is enabled in the corresponding instance.
- PIM-DM cannot be used for multicast groups in the SSM group range.

Related commands: **pim sm**; **ssm-policy**; **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IP multicast routing, and enable PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

pim hello-option dr-priority

Syntax

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

View

Interface view

Default Level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description

Use the **pim hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

Examples

Set the router priority for DR election to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

pim hello-option holdtime

Syntax

pim hello-option holdtime *interval*

undo pim hello-option holdtime

View

Interface view

Default Level

2: System level

Parameters

interval: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 means that the PIM neighbor is always reachable.

Description

Use the **pim hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

Examples

Set the PIM neighbor timeout time to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

pim hello-option lan-delay

Syntax

pim hello-option lan-delay *interval*

undo pim hello-option lan-delay

View

Interface view

Default Level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use the **pim hello-option lan-delay** command to configure the LAN-delay time, namely the length of time the device waits between receiving a prune message and taking a prune action, on the current interface.

Use the **undo pim hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time to 500 milliseconds.

Related commands: **pim hello-option override-interval**, **hello-option override-interval**, **hello-option lan-delay**.

Examples

Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

pim hello-option neighbor-tracking

Syntax

pim hello-option neighbor-tracking

undo pim hello-option neighbor-tracking

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

Examples

Disable join suppression on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

pim hello-option override-interval

Syntax

pim hello-option override-interval *interval*

undo pim hello-option override-interval

View

Interface view

Default Level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use the **pim hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **pim hello-option lan-delay**, **hello-option lan-delay**, **hello-option override-interval**.

Examples

Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option override-interval 2000
```

pim holdtime assert

Syntax

pim holdtime assert *interval*

undo pim holdtime assert

View

Interface view

Default Level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use the **pim holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, **holdtime assert**.

Examples

Set the assert timeout time to 100 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime assert 100
```

pim holdtime join-prune

Syntax

pim holdtime join-prune *interval*

undo pim holdtime join-prune

View

Interface view

Default Level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use the **pim holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, **holdtime join-prune**.

Examples

Set the join/prune timeout time to 280 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

pim require-genid

Syntax

pim require-genid

undo pim require-genid

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim require-genid** command to enable rejection of hello messages without Generation_ID.

Use the **undo pim require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Examples

Enable VLAN-interface 100 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim require-genid
```

pim sm

Syntax

pim sm

undo pim sm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim sm** command to enable PIM-SM.

Use the **undo pim sm** command to disable PIM-SM.

By default, PIM-SM is disabled.

Note that this command can take effect only after IP multicast routing is enabled in the corresponding instance.

Related commands: **pim dm**; **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IP multicast routing, and enable PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

pim state-refresh-capable

Syntax

pim state-refresh-capable

undo pim state-refresh-capable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, **state-refresh-ttl**.

Examples

Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

pim timer graft-retry

Syntax

pim timer graft-retry *interval*

undo pim timer graft-retry

View

Interface view

Default Level

2: System level

Parameters

interval: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description

Use the **pim timer graft-retry** command to configure the graft retry period.

Use the **undo pim timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

Examples

Set the graft retry period to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer graft-retry 80
```

pim timer hello

Syntax

pim timer hello *interval*

undo pim timer hello

View

Interface view

Default Level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **pim timer hello** command to configure on the current interface the interval at which hello messages are sent.

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

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

Examples

Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer hello 40
```

pim timer join-prune

Syntax

pim timer join-prune *interval*

undo pim timer join-prune

View

Interface view

Default Level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **pim timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

Examples

Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer join-prune 80
```

pim triggered-hello-delay

Syntax

pim triggered-hello-delay *interval*

undo pim trigged-hello-delay

View

Interface view

Default Level

2: System level

Parameters

interval: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

Description

Use the **pim triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim triggered-hello-delay** command to restore the system default.

By default, the maximum delay between hello messages is 5 seconds.

Examples

Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim trigged-hello-delay 3
```

probe-interval (PIM view)

Syntax

probe-interval *interval*

undo probe-interval

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Register probe time in seconds, with an effective range of 1 to 1799.

Description

Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the system default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples

Set the register probe time to 6 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] probe-interval 6
```

register-policy (PIM view)

Syntax

register-policy *acl-number*

undo register-policy

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

acl-number: Advanced ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the ACL can be accepted by the RP.

Description

Use the **register-policy** command to configure an ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

Examples

In the public instance configure the RP to accept only those register messages from multicast sources on the subnet of 10.10.0.0/16 for multicast groups on the subnet of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

register-suppression-timeout (PIM view)

Syntax

register-suppression-timeout *interval*

undo register-suppression-timeout

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Register suppression time in seconds, in the range of 1 to 3,600.

Description

Use the **register-suppression-timeout** command to configure the register suppression time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval**, **register-policy**.

Examples

Set the register suppression time to 70 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

register-whole-checksum (PIM view)

Syntax

register-whole-checksum

undo register-whole-checksum

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

None

Description

Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based on the header in the register message.

Related commands: **register-policy**, **register-suppression-timeout**.

Examples

Configure the router to calculate the checksum based on the entire register message in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

reset pim control-message counters

Syntax

reset pim [**all-instance** | **vpn-instance** *vpn-instance-name*] **control-message counters** [**interface** *interface-type interface-number*]

View

User view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

interface *interface-type interface-number*: Specifies to reset the PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information of PIM control messages on all interfaces.

Description

Use the **reset pim control-message counters** command to reset PIM control message counters.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will reset PIM control message counters on the public instance.

Examples

Reset PIM control message counters on all interfaces in the public instance.

```
<Sysname> reset pim control-message counters
```

source-lifetime (PIM view)

Syntax

source-lifetime *interval*

undo source-lifetime

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Multicast source lifetime in seconds, with an effective range of 1 to 65,535.

Description

Use the **source-lifetime** command to configure the multicast source lifetime.

Use the **undo source-lifetime** command to restore the system default.

By default, the lifetime of a multicast source is 210 seconds.

Examples

Set the multicast source lifetime to 200 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200
```

source-policy (PIM view)

Syntax

source-policy *acl-number*

undo source-policy

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999.

Description

Use the **source-policy** command to configure a multicast data filter.

Use the **undo source-policy** command to remove the configured multicast data filter.

By default, no multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Examples

In the public instance configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

spt-switch-threshold infinity (PIM view)

Syntax

spt-switch-threshold infinity [**group-policy** *acl-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl-number*]

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

group-policy *acl-number*: Specifies a basic ACL, in the range of 2000 to 2999. If you do not include this option in your command, the configuration will apply on all multicast groups.

order *order-value*: Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the ACL will remain the same in the group-policy list.

Description

Use the **spt-switch-threshold infinity** command to configure disabling the SPT switchover.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first multicast packet.

Note that:

- To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list will remain unchanged.
- To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence will take effect.
- For an S7900E series Ethernet switch, once a multicast forwarding entry is created, subsequent multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not use **spt-switch-threshold infinity** command on a switch that may become an RP (namely, a static RP or a C-RP).

Examples

Disable SPT switchover on a switch that will never become an RP.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

ssm-policy (PIM view)

Syntax

ssm-policy *acl-number*

undo ssm-policy

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999.

Description

Use the **ssm-policy** command to configure the SSM multicast group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the SSM group range is 232.0.0.0/8.

This command allows you to define an address range of permitted or denied multicast groups. If the match succeeds, the multicast mode will be PIM-SSM; otherwise the multicast mode will be PIM-SM.

Examples

Configure the SSM group range to be 232.1.0.0/16 in the public instance.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

state-refresh-interval (PIM view)

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: State refresh interval in seconds, with an effective range of 1 to 255.

Description

Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim state-refresh-capable**, **state-refresh-rate-limit**, **state-refresh-ttl**.

Examples

Set the state refresh interval to 70 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

state-refresh-rate-limit (PIM view)

Syntax

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description

Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, **state-refresh-ttl**.

Examples

In the public instance configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

state-refresh-ttl

Syntax

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

ttl-value: TTL value of state refresh messages, in the range of 1 to 255.

Description

Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the system default.

By default, the TTL value of state refresh messages is 255.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, **state-refresh-rate-limit**.

Examples

In the public instance configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

static-rp (PIM view)

Syntax

static-rp *rp-address* [*acl-number*] [**preferred**]

undo static-rp *rp-address*

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

rp-address: IP address of the static RP to be configured. This address must be a legal unicast IP address, rather than an address on the 127.0.0.0/8 segment.

acl-number: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those groups that pass the ACL filtering; otherwise, the configured static RP will serve the all-system group 224.0.0.0/4.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

Description

Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- PIM-SM or PIM-DM cannot be enabled on an interface that serves as a static RP.

- When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.
- You can configure multiple static RPs by using this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same multicast group, the one with the highest IP address will be chosen to serve the multicast group.
- You can configure up to 50 static RPs on the same device.

Related commands: **display pim rp-info**, **auto-rp enable**.

Examples

In the public instance, configure the interface with the IP address 11.110.0.6 to be a static RP that serves the multicast groups defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

timer hello (PIM view)

Syntax

timer hello *interval*

undo timer hello

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **timer hello** command to configure the hello interval globally.

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

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim timer hello**.

Examples

Set the global hello interval to 40 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

timer join-prune (PIM view)

Syntax

timer join-prune *interval*

undo timer join-prune

View

Public instance PIM view, VPN instance PIM view

Default Level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim timer join-prune**.

Examples

Set the global join/prune interval to 80 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

Table of Contents

1 MSDP Configuration Commands

Note

The term “router” in this document refers to a router in the generic sense or a Layer 3 switch running MSDP.

MSDP Configuration Commands

cache-sa-enable

Syntax

cache-sa-enable

undo cache-sa-enable

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

None

Description

Use the **cache-sa-enable** command to enable the SA cache mechanism to cache the (S, G) entries contained in SA messages.

Use the **undo cache-sa-enable** command to disable the SA cache mechanism.

By default, the SA cache mechanism is enabled, that is, the device caches the (S, G) entries contained in SA messages received.

Examples

Enable the SA message cache mechanism in the public instance so that the device caches the (S, G) entries contained in SA messages received.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

display msdp brief

Syntax

display msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

state: Displays the information of MSDP peers in the specified state.

connect: Displays the information of MSDP peers in the connecting state.

down: Displays the information of MSDP peers in the down state.

listen: Displays the information of MSDP peers in the listening state.

shutdown: Displays the information of MSDP peers in the deactivated state.

up: Displays the information of MSDP peers in the in-session state.

Description

Use the **display msdp brief** command to view the brief information of MSDP peers.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Examples

View the brief information of MSDP peers in all states in the public instance.

```
<Sysname> display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address    State    Up/Down time    AS     SA Count   Reset Count
  20.20.20.20       Up       00:00:13        100    0          0
```

Table 1-1 display msdp brief command output description

Field	Description
MSDP Peer Brief Information of VPN-Instance: public net	Brief information of MSDP peers of the public network
Configured	Number of MSDP peers configured
Up	Number of MSDP peers in the up state

Field	Description
Listen	Number of MSDP peers in the listen state
Connect	Number of MSDP peers in the connect state
Shutdown	Number of MSDP peers in the shutdown state
Down	Number of MSDP peers in the down state
Peer's Address	MSDP peer address
State	MSDP peer status: • Up: Session set up; MSDP peer in session • Listen: Session set up; local device as server, in listening state • Connect: Session not set up; local device as client, in connecting state • Shutdown: Deactivated • Down: Connection failed
Up/Down time	Length of time since MSDP peer connection was established/failed
AS	Number of the AS where the MSDP peer is located. “?” indicates that the system was unable to obtain the AS number.
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

display msdp peer-status

Syntax

display msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **peer-status** [*peer-address*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

peer-address: Specifies an MSDP peer by its address. If you do not provide this argument, this command will display the detailed status information of all MSDP peers.

Description

Use the **display msdp peer-status** command to view the detailed MSDP peer status information.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Related commands: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, **peer sa-request-policy**.

Examples

View the detailed status information of the MSDP peer with the address of 10.110.11.11 in the public instance.

```
<Sysname> display msdp peer-status 10.110.11.11
MSDP Peer Information of VPN-Instance: public net
     MSDP Peer 20.20.20.20, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (20.20.20.30)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
```

Table 1-2 display msdp peer-status command output description

Field	Description
MSDP Peer Information of VPN-Instance: public net	Information of the MSDP peer of the public network
MSDP Peer	MSDP peer address
AS	Number of the AS where the MSDP peer is located. “?” indicates that the system was unable to obtain the AS number.

Field	Description
State	MSDP peer status: • Up: Session set up; MSDP peer in session • Listen: Session set up; local device as server, in listening state • Connect: Session not set up; local device as client, in connecting state • Shutdown: Deactivated • Down: Connection failed
Resets	Number of times the MSDP peer connection is reset
Up/Down time	Length of time since MSDP peer connection was established/failed
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer
Number of sent/received messages	Number of SA messages sent and received through this connection
Number of discarded output messages	Number of discarded outgoing messages
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared
Information about (Source, Group)-based SA filtering policy	SA message filtering list information • Import policy: Filter list for receiving SA messages from the specified MSDP peer • Export policy: Filter list for forwarding SA messages from the specified MSDP peer
Information about SA-Requests	SA requests information • Policy to accept SA-Request messages: Filtering rule for receiving or forwarding SA messages from the specified MSDP peer • Sending SA-Requests status: Whether enabled to send an SA request message to the designated MSDP peer upon receiving a new Join message
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages
SAs learned from this peer	Number of cached (S, G) entries learned from this MSDP peer
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from this MSDP peer that the device can cache
Input queue size	Data size cached in the input queue
Output queue size	Data size cached in the output queue

Field	Description
Counters for MSDP message	MSDP peer statistics: • Count of RPF check failure: Number of SA messages discarded due to RPF check failure • Incoming/outgoing SA messages: Number of SA messages received and sent • Incoming/outgoing SA requests: Number of SA request received and sent • Incoming/outgoing SA responses: Number of SA responses received and sent • Incoming/outgoing data packets: Number of received and sent SA messages encapsulated with multicast data

display msdp sa-cache

Syntax

display msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address* | *source-address* | *as-number*] *

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Multicast group address in the (S, G) entry, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address in the (S, G) entry.

as-number: AS number, in the range of 1 to 65535.

Description

Use the **display msdp sa-cache** command to view the information of (S, G) entries in the SA cache.

Note that:

- If you do not specify all-instance nor vpn-instance, this command will display the information on the public instance.
- This command gives the corresponding output only after the **cache-sa-enable** command is executed.
- If you do not provide a group address, this command will display the (S, G) entry information for all multicast groups.
- If you do not provide a source address, this command will display the (S, G) entry information for all sources.

- If you provide neither a group address nor a source address, this command will display the information of all cached (S, G) entries.
- If you do not provide an AS number, this command will display the (S, G) entry information related to all ASs.

Related commands: **cache-sa-enable**.

Examples

View the information of (S, G) entries in the SA cache in the public instance.

```
<Sysname> display msdp sa-cache
MSDP Source-Active Cache Information of VPN-Instance: public net
 MSDP Total Source-Active Cache - 5 entries
 MSDP matched 5 entries

(Source, Group)              Origin RP       Pro  AS     Uptime   Expires
(10.10.1.2, 225.1.1.1)       10.10.10.10     BGP  100    00:00:11 00:05:49
(10.10.1.3, 225.1.1.1)       10.10.10.10     BGP  100    00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)       10.10.10.10     BGP  100    00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)       10.10.10.10     BGP  100    00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)       10.10.10.10     BGP  100    00:00:11 00:05:49
```

Table 1-3 display msdp sa-cache command output description

Field	Description
MSDP Source-Active Cache Information of VPN-Instance: public net	SA cache information of the public network
MSDP Total Source-Active Cache - 5 entries	Total number of (S, G) entries in the SA cache
MSDP matched 5 entries	Total number of (S, G) entries matched by MSDP
(Source, Group)	(S, G) entry: (source address, group address)
Origin RP	Address of the RP that generated the (S, G) entry
Pro	Type of protocol from which the AS number is originated. “?” indicates that the system was unable to obtain the protocol type.
AS	AS number of the origin RP. “?” indicates that the system was unable to obtain the AS number.
Uptime	Length of time for which the cached (S, G) entry has been existing, in hours:minutes:seconds
Expires	Length of time in which the cached (S, G) entry will expire, in hours:minutes:seconds

display msdp sa-count

Syntax

display msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **sa-count** [*as-number*]

View

Any view

Default Level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

as-number: AS number, in the range of 1 to 65535.

Description

Use the **display msdp sa-count** command to view the number of (S, G) entries in the SA cache.

Note that:

- If neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.
- This command gives the corresponding output only after the **cache-sa-enable** command is executed.

Related commands: **cache-sa-enable**.

Examples

View the number of (S, G) entries in the SA cache for the public instance.

```
<Sysname> display msdp sa-count
MSDP Source-Active Count Information of VPN-Instance: public net
  Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3

  Total 5 Source-Active entries
```

Table 1-4 display msdp sa-count command output description

Field	Description
MSDP Source-Active Count Information of VPN-Instance: public net	Number of SA messages for the public network cache
Number of cached Source-Active entries, counted by Peer	Number of (S, G) entries counted by peer
Peer's Address	Address of the MSDP peer that sent SA messages
Number of SA	Number of (S, G) entries from this peer
Number of source and group, counted by AS	Number of cached (S, G) entries, counted by AS

Field	Description
AS	AS number. “?” indicates that the system was unable to obtain the AS number.
Number of source	Number of multicast sources from this AS
Number of group	Number of multicast groups from this AS

encap-data-enable

Syntax

encap-data-enable

undo encap-data-enable

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

None

Description

Use the **encap-data-enable** command to enable register message encapsulation in SA messages.

Use the **undo encap-data-enable** command to disable register message encapsulation in SA messages.

By default, an SA message contains only an (S, G) entry. No register message is encapsulated in an SA message.

Examples

Enable register message encapsulation in SA messages in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

import-source

Syntax

import-source [**acl** *acl-number*]

undo import-source

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. A basic ACL is used to filter multicast sources, while an advanced ACL is used to filter multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information will be advertised.

Note

During ACL matching, the protocol ID in the ACL rule is not checked.

Description

Use the **import-source** command to configure a rule of creating (S, G) entries.

Use the **undo import-source** command to remove any rule of creating (S, G) entries.

By default, when an SA message is created, there are no restrictions on the (S, G) entries to be advertised in it, namely all the (S, G) entries within the domain are advertised in the SA message.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

Related commands: **peer sa-policy**.

Examples

Configure the MSDP peer in the public instance to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

msdp

Syntax

msdp [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

Description

Use the **msdp** command to enable MSDP in the public instance or the specified VPN instance and enter public instance or VPN instance MSDP view.

Use the **undo msdp** command to disable MSDP in the public instance or the specified VPN instance and remove the configurations performed in public instance or VPN instance MSDP view to free the resources occupied by MSDP.

By default, MSDP is disabled.

Note that:

- If you do not specify **vpn-instance**, this configuration will take effect only on the public instance
- IP multicast must be enabled in the corresponding instance before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands* of the *Multicast Volume*.

Examples

Enable IP multicast routing in the public instance, and enable MSDP in the public instance to enter public instance MSDP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] msdp
[Sysname-msdp]
```

Enable IP multicast routing in VPN instance mvpn, and enable MSDP in VPN instance mvpn to enter MSDP view of VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn]route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn]
```

originating-rp

Syntax

originating-rp *interface-type interface-number*

undo originating-rp

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

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

Description

Use the **originating-rp** command to configure the address of the specified interface as the RP address of SA messages.

Use the **undo originating-rp** command to restore the system default.

Be default, the PIM RP address is used as the RP address of SA messages.

Examples

Specify the IP address of VLAN-interface 100 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp vlan-interface 100
```

peer connect-interface

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

interface-type interface-number: Specifies an interface by its type and number. The local device will use the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Description

Use the **peer connect-interface** command to create an MSDP peer connection.

Use the **undo peer connect-interface** command to remove an MSDP peer connection.

No MSDP peer connection is created by default.

Be sure to carry out this command before you use any other **peer** command; otherwise the system will prompt that the peer does not exist.

Related commands: **static-rpf-peer**.

Examples

Configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local router, with interface VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

peer description

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

text: Descriptive string of 1 to 80 case sensitive characters including spaces.

Description

Use the **peer description** command to configure the description information for the specified MSDP peer.

Use the **undo peer description** command to delete the configured description information of the specified MSDP peer.

By default, an MSDP peer has no description information.

Related commands: **display msdp peer-status**.

Examples

In the public instance, add the descriptive text “Router CstmrA” for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description Router CstmrA
```

peer mesh-group

Syntax

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

name: Mesh group name, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any space.

Description

Use the **peer mesh-group** command to configure an MSDP peer as a mesh group member.

Use the **undo peer mesh-group** command to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

Examples

In the public instance, configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group “Grp1”.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Grp1
```

peer minimum-ttl

Syntax

peer *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

ttl-value: Time-to-Live (TTL) threshold, in the range of 0 to 255.

Description

Use the **peer minimum-ttl** command to configure the TTL threshold for multicast data packet encapsulation in SA messages.

Use the **undo peer minimum-ttl** command to restore the system default.

By default, the TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

Related commands: **display msdp peer-status**.

Examples

In the public instance, set the TTL threshold for multicast packets to be encapsulated in SA messages to 10 so that only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer request-sa-enable

Syntax

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

Description

Use the **peer request-sa-enable** command to enable the device to send an SA request message to the specified MSDP peer upon receiving a new join message.

Use the **undo peer request-sa-enable** command to disable the device from sending an SA request message to the specified MSDP peer.

By default, upon receiving a new join message, the router does not send an SA request message to any MSDP peer; instead, it waits for the next SA message to come.

Note that before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related commands: **cache-sa-enable**.

Examples

Disable the SA message cache mechanism in the public instance, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 upon receiving a new Join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

peer sa-cache-maximum

Syntax

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

sa-limit: Maximum number of (S, G) entries that the device can cache, in the range of 1 to 8,192.

Description

Use the **peer sa-cache-maximum** command to configure the maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.

Use the **undo peer sa-cache-maximum** command to restore the system default.

By default, the device can cache a maximum of 8,192 (S, G) entries learned from any MSDP peer.

Related commands: **display msdp sa-count**, **display msdp peer-status**, **display msdp brief**.

Examples

In the public instance allow the device to cache a maximum of 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

peer sa-policy

Syntax

peer *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** }

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

import: Specifies to filter SA messages from the specified MSDP peer.

export: Specifies to filter SA messages forwarded to the specified MSDP peer.

peer-address: MSDP peer address.

acl-number: Advanced ACL number, in the range of 3000 to 3999. If you do not provide an ACL number, all SA messages carrying (S, G) entries will be filtered off.

Description

Use the **peer sa-policy** command to configure a filtering rule for receiving or forwarding SA messages.

Use the **undo peer sa-policy** command to restore the default setting.

By default, SA messages received or to be forwarded are not filtered, namely, all SA messages are accepted or forwarded.

In addition to controlling SA message receiving and forwarding by using this command, you can also configure a filtering rule for creating SA messages using the **import-source** command.

Related commands: **display msdp peer-status**, **import-source**.

Examples

Configure a filtering rule so that SA messages will be forwarded to the MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax

peer *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

acl-number: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the SA requests of only the multicast groups that match the ACL will be accepted and other SA requests will be ignored; if you do not provide this argument, all SA requests will be ignored.

Description

Use the **peer sa-request-policy** command to configure a filtering rule for SA request messages.

Use the **undo peer sa-request-policy** command to remove the configured SA request filtering rule.

Be default, SA request messages are not filtered.

Related commands: **display msdp peer-status**.

Examples

Configure an SA request filtering rule in the public instance so that SA messages from the MSDP peer 175.58.6.5 will be accepted only if the multicast group address in the SA messages is in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax

reset msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **peer** [*peer-address*]

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

peer-address: Specifies an MSDP peer by its address. If you do not provide this argument, the TCP connections with all MSDP peers will be reset.

Description

Use the **reset msdp peer** command to reset the TCP connection with the specified MSDP peer or the TCP connections with all MSDP peers and clear all the statistics information of the MSDP peer(s).

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

Related commands: **display msdp peer-status**.

Examples

Reset the TCP connection in the public instance with the MSDP peer 125.10.7.6 and clear all the statistics information of this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax

reset msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address*]

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

group-address: Specifies a multicast group, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide this argument, the command will clear the cached (S, G) entries for all multicast groups from the SA cache.

Description

Use the **reset msdp sa-cache** command to clear (S, G) entries from the SA cache.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will clear the information on the public instance.

Related commands: **cache-sa-enable**, **display msdp sa-cache**.

Examples

Clear the (S, G) entries for multicast group 225.5.4.3 from the SA cache of the public instance.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax

reset msdp [**all-instance** | **vpn-instance** *vpn-instance-name*] **statistics** [*peer-address*]

View

User view

Default Level

2: System level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.

peer-address: Address of the MSDP peer of which the statistics information is to be cleared. If you do not provide this argument, the command will clear the statistics information of all MSDP peers.

Description

Use the **reset msdp statistics** command to clear the statistics information of the specified MSDP peer or all MSDP peers without resetting the MSDP peer(s).

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will clear the information on the public instance.

Examples

Clear the statistics information of the MSDP peer 125.10.7.6 in the public instance.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP View)

Syntax

shutdown *peer-address*

undo shutdown *peer-address*

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

Description

Use the **shutdown** command to deactivate manually the connection with the specified MSDP peer.

Use the **undo shutdown** command to reactivate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related commands: **display msdp peer-status**.

Examples

Deactivate the connection with the MSDP peer 125.10.7.6 in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

static-rpf-peer

Syntax

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

peer-address: MSDP peer address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a case sensitive string of 1 to 19 characters. A policy name must not contain any space.

Description

Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the follow rules:

1) If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers take effect concurrently. SA messages will be filtered as per the configured prefix list and only those SA messages whose RP addresses pass the filtering will be accepted. If multiple static RPF peers use the same filtering policy at the same time, when a peer receives an SA message, it will forward the SA message to the other peers.
2) If you use the **rp-policy** keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in the UP state will be activated, and all SA messages from this peer will be accepted while the SA messages from other static RPF peers will be discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), still the first RPF peer whose connection is in UP state will be selected as the activated RPF peer according to the configuration sequence.

Related commands: **display msdp peer-status**, **ip prefix-list**.

Examples

Configure static RPF peers.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax

timer retry *interval*

undo timer retry

View

Public instance MSDP view, VPN instance MSDP view

Default Level

2: System level

Parameters

interval: Interval between MSDP peer connection retries, in seconds. The effective range is 1 to 60.

Description

Use the **timer retry** command to configure the interval between MSDP peer connection retries.

Use the **undo timer retry** command to restore the default setting.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related commands: **display msdp peer-status**.

Examples

Set the MSDP peer connection retry interval to 60 seconds in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] timer retry 60
```

Table of Contents

1 MBGP Configuration Commands

Note

- The term “router” in this document refers to a generic router or an Ethernet switch running routing protocols.
- For information about route policy commands, refer to *Route Policy Commands* in the *IP Routing Volume*.

MBGP Configuration Commands

aggregate (MBGP family view)

Syntax

aggregate *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* | *mask-length* }

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

ip-address: Summary address.

mask: Summary mask, in dotted decimal notation.

mask-length: Summary mask length, in the range 0 to 32.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name:* Sets the attributes of the summary route according to the route policy. The route policy name is a string of 1 to 19 characters.

detail-suppressed: Advertises the summary route only.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the route policy. The route policy name is a string of 1 to 19 characters.

origin-policy *route-policy-name*: References the route policy to determine routes for summarization. The route policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

Table 1-1 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route flaps.
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the **peer filter-policy** command.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the **if-match** clause of the **route-policy** command.
origin-policy	Selects only routes satisfying the route policy for route summarization
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the **peer route-policy** command.

Description

Use the **aggregate** command to create a summary route in the IPv4 MBGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

Examples

In IPv4 MBGP address family view, create a summary of 192.213.0.0/16 in the IPv4 MBGP routing table.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]aggregate 10.40.0.0 255.255.0.0
```

balance (MBGP family view)

Syntax

balance *number*

undo balance

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

number: Number of MBGP routes for load balancing, in the range 1 to 4. When it is set to 1, load balancing is disabled.

Description

Use the **balance** command to configure the number of MBGP routes for load balancing.

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

By default, no load balancing is configured.

Unlike IGP, MBGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by using route selection rules.

Related commands: **display ip multicast routing-table**.

Examples

In IPv4 MBGP address family view, set the number of routes for BGP load balancing to 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]balance 2
```

bestroute as-path-neglect (MBGP family view)

Syntax

bestroute as-path-neglect

undo bestroute as-path-neglect

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute as-path-neglect** command to configure MBGP not to consider the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to restore the default.

By default, MBGP considers AS_PATH during best route selection.

Examples

In IPv4 MBGP address family view, configure BGP to ignore the AS_PATH during best route selection.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul]bestroute as-path-neglect
```

bestroute compare-med (MBGP family view)

Syntax

bestroute compare-med

undo bestroute compare-med

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS during best route selection.

Use the **undo bestroute compare-med** command to disable this comparison.

The comparison is not enabled by default.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from each AS during best route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] bestroute compare-med
```

bestroute med-confederation (MBGP family view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] bestroute med-confederation
```

compare-different-as-med (MBGP family view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If several paths to one destination are available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP and routing selection method.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
```

```
[Sysname-bgp-af-mul]compare-different-as-med
```

dampening (MBGP family view)

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

half-life-reachable: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be greater than the *suppress* value. By default, the value is 16000.

route-policy-name: Route policy name, a string of 1 to 19 characters.

Description

Use the **dampening** command to configure IPv4 MBGP route dampening.

Use the **undo dampening** command to disable route dampening.

By default, no IPv4 MBGP route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

Examples

In IPv4 MBGP address family view, configure IPv4 MBGP route dampening.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]dampening 15 15 1000 2000 10000
```

default local-preference (MBGP family view)

Syntax

default local-preference *value*

undo default local-preference

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

value: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default local preference is 100.

Using this command can affect MBGP route selection.

Examples

In IPv4 MBGP address family view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]default local-preference 180
```

default med (MBGP family view)

Syntax

default med *med-value*

undo default med

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

med-value: Default MED value, in the range 0 to 4294967295.

Description

Use the **default med** command to specify the default MED value.

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

By default, the default MED value is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is

preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system selects the route with the smallest MED as the best external route.

Examples

In IPv4 MBGP address family view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]default med 25
```

default-route imported (MBGP family view)

Syntax

default-route imported

undo default-route imported

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **default-route imported** command to allow default route redistribution into the MBGP routing table.

Use the **undo default-route imported** command to restore the default.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route.**

Examples

In IPv4 MBGP address family view, allow default route redistribution from OSPF into MBGP.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] default-route imported
[Sysname-bgp-af-mul] import-route ospf 1
```

display ip multicast routing-table

Syntax

display ip multicast routing-table [**verbose**]

View

Any view

Default Level

2: Monitor level

Parameters

verbose: Displays the detailed information of the multicast routing table, including both inactive and active multicast routes. Without the keyword, the command displays brief information about only the active MBGP routes.

Description

Use the **display ip multicast routing-table** command to display the multicast BGP routing table.

All the active MBGP routes in the MBGP routing table are used for RPF check, but inactive MBGP routes are not.

Examples

Display brief information about the active routes in the multicast BGP routing table.

```
<Sysname> display ip multicast routing-table
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

2.2.2.0/24          Direct 0    0            2.2.2.1         Vlan-interface2
2.2.2.1/32          Direct 0    0            127.0.0.1       InLoopBack0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoopBack0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoopBack0
192.168.80.0/24     Direct 0    0            192.168.80.10   Vlan-interface1
192.168.80.10/32    Direct 0    0            127.0.0.1       InLoopBack0
```

Table 1-2 display ip multicast routing-table command output description

Field	Description
Destinations	Number of destinations
Routes	Number of routes
Destination/Mask	Destination address /Mask length
Proto	Routing protocol that discovered the route
Pre	Route preference
Cost	Route cost
Nexthop	Next hop of the route

Field	Description
Interface	Outgoing interface to reach the destination

Display the detailed information of the multicast routing table.

```
<Sysname> display ip multicast routing-table verbose
Routing Table : Public
        Destinations : 2        Routes : 2

Destination: 192.168.80.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 192.168.80.10    Interface: Vlan-interface1
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h14m49s
          Tag: 0

Destination: 192.168.80.10/32
     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: 00h14m49s
          Tag: 0
```

Table 1-3 display ip multicast routing-table verbose command output description

Field	Description
Destination	Destination/mask
Protocol	Routing protocol that discovered the route
Process ID	Process ID
Preference	Route preference
Cost	Route cost
NextHop	Nexthop of the route
Interface	Outgoing interface to reach the destination
RelyNextHop	Recursive next hop
Neighbour	Neighbor address
Tunnel ID	Tunnel ID
Label	Label
State	Route state: Active, Inactive, Adv (can be advertised), NoAdv (cannot be advertised)
Age	Age of the route, in the sequence of hour, minute, and second from left to right.

Field	Description
Tag	Route tag

display ip multicast routing-table *ip-address*

Syntax

display ip multicast routing-table *ip-address* [*mask-length* |*mask*] [**longer-match**] [**verbose**]

View

Any view

Default Level

2: 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 information about both active and inactive routes. With this argument absent, the command displays only brief information about active routes.

Description

Use the **display ip multicast routing-table** command to display information about multicast routes to a specified destination address.

Executing the command with different parameters yields different outputs:

display ip multicast routing-table *ip-address*

It displays all multicast routes falling into the natural network of the IP address. If no such multicast routes are available, it displays only the longest matched active multicast route.

display ip multicast routing-table *ip-address mask*

It displays the multicast route exactly matching the IP address and mask.

Examples

Display brief information about all multicast routes falling into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 169.0.0.0
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost  NextHop         Interface
169.0.0.0/16        Static  60    0    2.1.1.1          LoopBack1
```

Display brief information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.0.0
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost  NextHop         Interface
169.0.0.0/8         Static 60    0    2.1.1.1         LoopBack1
```

Display detailed information about multicast routes falling into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 2.2.2.1 verbose
Routing Table : Public
Summary Count : 1

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: 05h38m46s
          Tag: 0
```

Display detailed information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.2.1 verbose
Routing Table : Public
Summary Count : 1

Destination: 169.0.0.0/8
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 169.1.1.1        Interface: Vlan-interface1
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h00m32s
          Tag: 0
```

display bgp multicast group

Syntax

display bgp multicast group [*group-name*]

View

Any view

Default Level

2: Monitor level

Parameters

group-name: MBGP peer group name, a string of 1 to 47 characters.

Description

Use the **display bgp multicast group** command to display IPv4 MBGP peer group information.

Examples

Display the information of the IPv4 MBGP peer group **aaa**.

```
<Sysname> display bgp multicast group aaa
 BGP peer-group is aaa
 remote AS 200
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  2.2.2.1         4   200        0        0     0       0 00:00:35 Active
```

Table 1-4 display bgp multicast group command output description

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisement
Peer Preferred Value	Preferred value specified for the routes from the peer
No routing policy is configured	No route policy is configured.
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on the peer

Field	Description
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	Time elapsed
State	State machine of the peer

display bgp multicast network

Syntax

display bgp multicast network

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast network** command to display IPv4 MBGP routing information advertised with the **network** command.

Examples

Display IPv4 MBGP routing information advertised with the **network** command.

```
<Sysname> display bgp multicast network
  BGP Local Router ID is 10.1.4.2.
  Local AS Number is 400.
  Network          Mask            Route-policy        Short-cut

  100.1.2.0        255.255.255.0
  100.1.1.0        255.255.255.0                       Short-cut
```

Table 1-5 display bgp multicast network command output description

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Mask	Mask

Field	Description
Route-policy	Route policy referenced
Short-cut	Short-cut route

display bgp multicast paths

Syntax

display bgp multicast paths [*as-regular-expression*]

View

Any view

Default Level

2: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 case-sensitive characters, including spaces.

Description

Use the **display bgp multicast paths** command to display the AS path information of IPv4 MBGP routes.

Examples

Display the AS path information of IPv4 MBGP routes.

```
<Sysname> display bgp multicast paths ^200

   Address       Hash    Refcount  MED         Path/Origin
   0x5917100     11      1                     200 300i
```

Table 1-6 display bgp multicast paths command output description

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that reference the path
MED	MED of the path
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops

Field	Description	
Origin	Origin attribute of the path:	
	i	Indicates the route is interior to the AS. Summary routes and routes injected using the **network** command are considered IGP routes.
	e	Indicates the route is learned from the Exterior Gateway Protocol (EGP).
	?	Indicates the origin of the route is unknown. Routes redistributed from other routing protocols have this origin attribute.

display bgp multicast peer

Syntax

display bgp multicast peer [*ip-address*] [**verbose**]

View

Any view

Default Level

2: Monitor level

Parameters

ip-address: IP address of an IPv4 MBGP peer to be displayed, in dotted decimal notation.

verbose: Displays the detailed information of the peer/peer group.

Description

Use the **display bgp multicast peer** command to display IPv4 MBGP peer information.

Examples

Display the detailed information of the IPv4 MBGP peer 10.110.25.20.

```
<Sysname> display bgp multicast peer 10.110.25.20 verbose

          Peer: 10.110.25.20 Local: 2.2.2.2
          Type: EBGP link
          BGP version 4, remote router ID 1.1.1.1
          BGP current state: Established, Up for 00h01m51s
          BGP current event: RecvKeepalive
          BGP last state: OpenConfirm
          Port:  Local - 1029     Remote - 179
          Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
          Received  : Active Hold Time: 180 sec
          Negotiated: Active Hold Time: 180 sec
          Peer optional capabilities:
          Peer support bgp multi-protocol extended
          Peer support bgp route refresh capability
```

```
        Address family IPv4 Unicast: advertised and received

Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0
BFD: Enabled

Routing policy configured:
No routing policy is configured
```

Table 1-7 display bgp multicast peer command output description

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type
BGP version	BGP version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Previous state of the peer
Port	TCP port numbers
Configured: Active Hold Time	Local holdtime interval
Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval
Peer optional capabilities	Optional capabilities supported by the peer, including multiprotocol BGP extensions and route refresh
Address family IPv4 Unicast	Routes are advertised and received in IPv4 unicasts.
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer
BFD	Status of BGP (enabled/disabled)

Field	Description
Routing policy configured	Local route policy

display bgp multicast routing-table

Syntax

display bgp multicast routing-table [*ip-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-prefixes: Matches the longest prefix.

Description

Use the **display bgp multicast routing-table** command to display IPv4 MBGP routing information.

Examples

Display the IPv4 MBGP routing table.

```
<Sysname> display bgp multicast routing-table

 Total Number of Routes: 1

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  40.40.40.0/24     20.20.20.1                              0       200 300i
```

Table 1-8 display bgp multicast routing-table command output description

Field	Description
Total Number of Routes	Total Number of Routes
BGP Local router ID	BGP local router ID

Field	Description	
Status codes	Status codes: * – valid > – best d – damped h – history i – internal s – suppressed S – Stale	
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by some other means)	
Network	Destination network address	
Next Hop	Next hop	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
PrefVal	Preferred value of the route	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
Ogn	Origin attribute of the route, which can be one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes injected with the **network** command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by some other means. BGP marks routes redistributed from IGP as incomplete.

display bgp multicast routing-table as-path-acl

Syntax

display bgp multicast routing-table as-path-acl *as-path-acl-number*

View

Any view

Default Level

2: Monitor level

Parameters

as-path-acl-number: Displays IPv4 MBGP routing information matching the AS path ACL, which is specified with a number from 1 to 256.

Description

Use the **display bgp multicast routing-table as-path-acl** command to display IPv4 MBGP routes matching an AS-path ACL.

Examples

Display IPv4 MBGP routes matching AS path ACL 1.

```
<Sysname> display bgp multicast routing-table as-path-acl 1

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf      PrefVal Path/Ogn

*>  40.40.40.0/24     30.30.30.1     0                    0      300i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table cidr

Syntax

display bgp multicast routing-table cidr

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast routing-table cidr** command to display IPv4 MBGP Classless Inter-Domain Routing (CIDR) routing information.

Examples

Display IPv4 MBGP CIDR routing information.

```
<Sysname> display bgp multicast routing-table cidr

Total Number of Routes: 1

 BGP Local router ID is 20.20.20.1
```

```
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop         MED        LocPrf     PrefVal Path/Ogn

*>  40.40.40.0/24    30.30.30.1      0                     0       300i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table community

Syntax

display bgp multicast routing-table community [*aa:nn*]&<1-13> [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View

Any view

Default Level

2: Monitor level

Parameters

aa:nn: Community number. Both aa and nn are in the range 0 to 65535.

&<1-13>: Argument before it can be entered up to 13 times.

no-advertise: Displays MBGP routes that cannot be advertised to any peer.

no-export: Displays MBGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays MBGP routes that cannot be advertised out the AS or to other sub ASs in the confederation.

whole-match: Displays the MBGP routes exactly matching the specified community attributes.

Description

Use the **display bgp multicast routing-table community** command to display IPv4 MBGP routing information with the specified BGP community attribute.

Examples

Display IPv4 MBGP routing information with the specified BGP community attribute.

```
<Sysname> display bgp multicast routing-table community 11:22

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  10.10.10.0/24     0.0.0.0         0                     0      i
```

```
*>  40.40.40.0/24      20.20.20.1                              0       200 300i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table community-list

Syntax

display bgp multicast routing-table community-list { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View

Any view

Default Level

2: Monitor level

Parameters

basic-community-list-number: Specifies a basic community-list number from 1 to 99.

adv-community-list-number: Specifies an advanced community-list number from 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

Description

Use the **display bgp multicast routing-table community-list** command to display IPv4 MBGP routing information matching the specified BGP community list.

Examples

Display MBGP routing information matching the community list 100.

```
<Sysname> display bgp multicast routing-table community-list 100
 BGP Local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
      Network            NextHop        Metric     LocPrf    PrefVal Path

 *>   3.3.3.0/30         1.2.3.4                               0       ?
 *>   4.4.0.0/20         1.2.3.4                               0       ?
 *>   4.5.6.0/26         1.2.3.4                               0       ?


 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn
 *>  30.30.30.0/24     0.0.0.0       0                    0       i
 *>  40.40.40.0/24     0.0.0.0       0                    0       i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table dampened

Syntax

display bgp multicast routing-table dampened

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast routing-table dampened** command to display dampened IPv4 MBGP routes.

Examples

Display dampened IPv4 MBGP routes.

```
<Sysname> display bgp multicast routing-table dampened
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            From              Reuse     Path/Origin
 *d  77.0.0.0           12.1.1.1          00:29:20  100?
```

Table 1-9 display bgp multicast routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to Table 1-8 for description on the other fields above.

display bgp multicast routing-table dampening parameter

Syntax

display bgp multicast routing-table dampening parameter

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast routing-table dampening parameter** command to display IPv4 MBGP route dampening parameters.

Related commands: **dampening**.

Examples

Display IPv4 MBGP route dampening parameters.

```
<Sysname> display bgp multicast routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
Ceiling Value                    : 16000
 Reuse Value                      : 750
 Reach HalfLife Time(in  second)  : 900
 Unreach HalfLife Time(in  second): 900
 Suppress-Limit                   : 2000
```

Table 1-10 display bgp multicast routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
HalfLife Time	Half-life time of active routes
Suppress-Limit	Threshold at which a route is suppressed

display bgp multicast routing-table different-origin-as

Syntax

display bgp multicast routing-table different-origin-as

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast routing-table different-origin-as** command to display IPv4 MBGP routes originating from different autonomous systems.

Examples

Display IPv4 MBGP routes originating from different autonomous systems.

```
<Sysname> display bgp multicast routing-table different-origin-as
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  55.0.0.0         12.1.1.1       0                   0       100?
 *                   14.1.1.2       0                   0       300?
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table flap-info

Syntax

display bgp multicast routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* } [**longer-match**]]]

View

Any view

Default Level

2: Monitor level

Parameters

as-regular-expression: Displays route flap information that matches the AS path regular expression.

as-path-acl-number: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-match: Matches the longest prefix.

Description

Use the **display bgp multicast routing-table flap-info** command to display IPv4 MBGP route flap statistics. If no parameter is specified, this command displays all IPv4 MBGP route flap statistics.

Examples

Display IPv4 MBGP route flap statistics.

```
<Sysname> display bgp multicast routing-table flap-info

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network        From        Flaps  Duration   Reuse     Path/Origin

 *>  55.0.0.0       12.1.1.1    2      00:00:16             100?
 *d  77.0.0.0       12.1.1.1    5      00:34:02   00:27:08  100?
```

Table 1-11 display bgp multicast routing-table flap-info command output description

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Route flap duration
Reuse	Reuse time of the route

Refer to Table 1-8 for description on the other fields above.

display bgp multicast routing-table peer

Syntax

display bgp multicast routing-table peer *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistic**]

View

Any view

Default Level

2: Monitor level

Parameters

ip-address: IP address of an IPv4 MBGP peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

statistic: Displays route statistics.

Description

Use the **display bgp multicast routing-table peer** command to display IPv4 MBGP routing information advertised to or received from the specified IPv4 MBGP peer.

Related commands: display bgp multicast peer.

Examples

Display IPv4 MBGP routing information advertised to the peer 20.20.20.1.

```
<Sysname> display bgp multicast routing-table peer 20.20.20.1 advertised-routes

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  30.30.30.0/24     0.0.0.0        0                   0       i
 *>  40.40.40.0/24     0.0.0.0        0                   0       i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table regular-expression

Syntax

display bgp multicast routing-table regular-expression *as-regular-expression*

View

Any view

Default Level

2: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 case-sensitive characters, including spaces.

Description

Use the **display bgp multicast routing-table regular-expression** command to display IPv4 MBGP routing information matching the specified AS path regular expression.

Examples

Display IPv4 MBGP routing information matching AS path regular expression 300$.

```
<Sysname> display bgp multicast routing-table regular-expression 300$

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn
```

```
 *>  40.40.40.0/24     30.30.30.1    0                      0       300i
```

Refer to Table 1-8 for description on the fields above.

display bgp multicast routing-table statistic

Syntax

display bgp multicast routing-table statistic

View

Any view

Default Level

2: Monitor level

Parameters

None

Description

Use the **display bgp multicast routing-table statistic** command to display IPv4 MBGP routing statistics.

Examples

Display IPv4 MBGP routing statistics.

```
<Sysname> display bgp multicast routing-table statistic

 Total Number of Routes: 4
```

Table 1-12 display bgp multicast routing-table statistic command output description

Field	Description
Total Number of Routes	Total Number of Routes

filter-policy export (MBGP family view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing routing information, a string of 1 to 19 characters.

direct: Filters direct routes.

isis *process-id*: Filters outgoing routes redistributed from an ISIS process. The process ID is in the range 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The process ID is in the range 1 to 65535.

static: Filters static routes.

Description

Use the **filter-policy export** command to configure the filtering of outgoing routes.

Use the **undo filter-policy export** command to remove the filtering.

By default, the filtering is not configured.

If no routing protocol is specified, all redistributed routes are filtered.

Examples

In IPv4 MBGP address family view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 export
```

filter-policy import (MBGP Family view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

acl-number: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

Examples

In IPv4 MBGP address family view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 import
```

import-route (MBGP family view)

Syntax

import-route *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

protocol: Redistributes routes from the routing protocol, which can be **direct**, **isis**, **nat**, **ospf**, **rip** or **static** at present.

process-id: Process ID, in the range 1 to 65535. It is available only when the protocol is **isis**, **ospf** or **rip**.

med-value: Specifies a MED value for redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of a redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a route policy used to filter redistributed routes, a string of 1 to 19 characters.

Description

Use the **import-route** command to enable route redistribution from a specified routing protocol.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, MBGP does not redistribute routes from other protocols.

The origin attribute of routes redistributed with the **import-route** command is incomplete.

Examples

In IPv4 MBGP address family view, enable route redistribution from RIP.

```
<Sysname> system-view
[Sysname]bgp 100
```

```
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] import-route rip
```

ipv4-family multicast

Syntax

ipv4-family multicast

undo ipv4-family multicast

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **ipv4-family multicast** command to enter IPv4 MBGP address family view.

Use the **undo ipv4-family multicast** command to remove all the settings made in IPv4 MBGP address family view.

Examples

Enter IPv4 MBGP address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul]
```

network (MBGP family view)

Syntax

network *ip-address* [*mask* | *mask-length*] [**short-cut** | **route-policy** *route-policy-name*]

undo network *ip-address* [*mask* | *mask-length*] [**short-cut**]

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

ip-address: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

short-cut: Specifies the route to use the local preference. If the route is an EBGP route whose preference is higher than the local preference, using this keyword can configure the EBGP route to use the local preference, and thus the route can hardly become the optimal route.

route-policy-name: Route policy applied to the route. The name is a string of 1 to 19 characters.

Description

Use the **network** command to inject a network to the IPv4 MBGP routing table.

Use the **undo network** command to remove a network from the IPv4 MBGP routing table.

By default, no network route is injected.

Note that:

- The network route to be injected must exist in the local IP routing table, and using a route policy makes route management more flexible.
- The origin attribute of the network route injected with the **network** command is IGP.

Examples

In IPv4 MBGP address family view, inject the network 10.0.0.0/16.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] network 10.0.0.1 255.255.0.0
```

peer advertise-community (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list, if-match community**, **apply community** (refer to *Route policy Commands* in the *IP Routing Volume*).

Examples

In IPv4 MBGP address family view, advertise the community attribute to the existing peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-community
```

peer advertise-ext-community (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **advertise-ext-community**

undo peer { *group-name* | *ip-address* } **advertise-ext-community**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the extended community attribute advertisement to a peer/peer group.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to the **ip extcommunity-list**, **if-match extcommunity** and **apply extcommunity** commands in *Route policy Commands* of the *IP Routing Volume*.

Examples

In IPv4 MBGP address family view, advertise the extended community attribute to the existing peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-ext-community
```

peer allow-as-loop (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

number: Specifies the number of times the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the number of times the local AS number can appear.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is not allowed.

Related commands: display bgp multicast routing-table peer.

Examples

In IPv4 MBGP address family view, configure the number of times the local AS number can appear in routes from the peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 1.1.1.1 enable
[Sysname-bgp-af-mul] peer 1.1.1.1 allow-as-loop 2
```

peer as-path-acl (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

as-path-acl-number: AS path ACL number, in the range 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Description

Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the filtering.

By default, no AS path ACL based filtering is configured.

Related commands: **ip as-path**, **if-match as-path** and **apply as-path** (refer to *IP Route policy Commands* in the *IP Routing Volume*).

Examples

In IPv4 MBGP address family view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test as-path-acl 1 export
```

peer default-route-advertise (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ip-address* } **default-route-advertise**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

route-policy-name: Route policy name, a string of 1 to 19 characters.

Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples

In IPv4 MBGP address family view, advertise a default route to the existing peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test default-route-advertise
```

peer enable (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **enable**

undo peer { *group-name* | *ip-address* } **enable**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer enable** command to enable the specified peer/peer group that has been created in BGP view.

Use the **undo peer enable** command to disable the specified peer/peer group that has been created in BGP view.

If a peer is disabled, the router will not exchange routing information with the peer.

Examples

Enable the peer 18.10.0.9.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]peer 18.10.0.9 as-number 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 18.10.0.9 enable
```

peer filter-policy (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** [*acl-number*] { **export** | **import** }

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Uses the ACL to filter routes outgoing to the peer/peer group.

import: Uses the ACL to filter routes incoming from the peer/peer group.

Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the filtering.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

Examples

In IPv4 MBGP address family view, reference ACL 2000 to filter routes sent to the peer group test.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test filter-policy 2000 export
```

peer group (MBGP family view)

Syntax

peer *ip-address* **group** *group-name*

undo peer *ip-address* **group** *group-name*

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer group** command to add an IPv4 MBGP peer to an IPv4 MBGP peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

Examples

In IPv4 MBGP address family view, add the peer 10.1.1.1 to the multicast EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer 10.1.1.1 group test
```

peer ip-prefix (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

export: Applies the filter to routes outgoing to the specified peer/peer group.

import: Applies the filter to routes from the specified peer/peer group.

Description

Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list based filtering is configured.

Examples

In IPv4 MBGP address family view, use the IP prefix list **1** to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test ip-prefix list1 export
```

peer keep-all-routes (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **keep-all-routes**

undo peer { *group-name* | *ip-address* } **keep-all-routes**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, including routes that fail to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this feature.

By default, the feature is not enabled.

Examples

In IPv4 MBGP address family view, save all the routing information from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
```

```
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 keep-all-routes
```

peer next-hop-local (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer next-hop-local** command to specify the router as the next hop for routes sent to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes outgoing to an IBGP peer/peer group do not take the local router as the next hop.

Examples

In IPv4 MBGP address family view, specify the router as the next hop for routes sent to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test internal
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test next-hop-local
```

peer preferred-value (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

value: Preferred value, in the range 0 to 65535.

Description

Use the **peer preferred-value** command to specify a preferred value for routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value. Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the route to the destination.

Note that:

If you both reference a route policy and use the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command to set a preferred value for routes from a peer/peer group, the route policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the route policy uses the value set with the **peer preferred-value** command. If the preferred value specified in the route policy is zero, the routes matching it will also use the value set with the command.

For information about using a route policy to set a preferred value, refer to the command **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** } in this document, and the command **apply preferred-value** *preferred-value* in *Route policy Commands* of the *IP Routing Volume*.

Examples

In IPv4 MBGP address family view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, outgoing BGP updates can carry private AS numbers.

The command does not take effect for BGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

Examples

In IPv4 MBGP address family view, disable updates sent to the peer group **test** from carrying private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test public-as-only
```

peer reflect-client (MBGP family view)

Syntax

peer { *group-name* | *peer-address* } **reflect-client**

undo peer { *group-name* | *peer-address* } **reflect-client**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

peer-address: IP address of an IPv4 MBGP peer.

Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither the route reflector nor the client is configured.

Related commands: reflect between-clients and reflect cluster-id.

Examples

In IPv4 MBGP address family view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test internal
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test reflect-client
```

peer route-limit (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **route-limit** *limit* [*percentage*]

undo peer { *group-name* | *ip-address* } **route-limit**

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

limit: Upper limit of IP prefixes that can be received from the peer or peer group. Its range and default value vary with devices.

percentage: If the number of received routes divided by the upper limit reaches the specified percentage, the system will generate alarm information. The percentage is in the range 1 to 100. The default is 75.

Description

Use the **peer route-limit** command to set the maximum number of routes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is unlimited by default.

Examples

In IPv4 MBGP address family view, set the number of routes that can be received from peer 131.108.1.1 to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 route-limit 10000
```

peer route-policy (MBGP family view)

Syntax

peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

group-name: Peer group name, a string of 1 to 47 characters.

ip-address: IP address of an IPv4 MBGP peer.

route-policy-name: Route policy name, a string of 1 to 19 characters.

export: Applies the route policy to routes advertised to the peer/peer group.

import: Applies the route policy to routes received from the peer/peer group.

Description

Use the **peer route-policy** command to apply a route policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no route policy is applied to routes from/to the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced route policy. Refer to *Route policy Commands* in the *IP Routing Volume* for related commands.

Examples

In IPv4 MBGP address family view, apply the route policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
```

```
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test route-policy test-policy export
```

preference (MBGP family view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

external-preference: Preference of EBGP routes, in the range 1 to 255.

internal-preference: Preference of IBGP routes, in the range 1 to 255.

local-preference: Preference of local routes, in the range 1 to 255.

route-policy-name: Route policy name, a string of 1 to 19 characters. Using a route policy can set preferences for the routes matching it. As for the unmatched routes, the default preferences are adopted.

Description

Use the **preference** command to configure preferences for external, internal, and local routes.

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

The default preference values of external, internal and local BGP routes are 255, 255, and 130, respectively

Examples

In IPv4 MBGP address family view, configure preferences for EBGP, IBGP, and local IPv4 MBGP routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] preference 20 20 200
```

reflect between-clients (MBGP family view)

Syntax

reflect between-clients

undo reflect between-clients

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need to disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples

Disable route reflection between clients.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] undo reflect between-clients
```

reflector cluster-id (MBGP family view)

Syntax

reflector cluster-id { *cluster-id* | *ip-address* }

undo reflector cluster-id

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

cluster-id: Cluster ID of the route reflector, in the range 1 to 4294967295.

ip-address: Cluster ID of the route reflector, in the format of an IP address.

Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

A route is reflected by a route reflector from a client to another client. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a

cluster has multiple route reflectors, you need to use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

Examples

Specify 80 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] reflector cluster-id 80
```

refresh bgp ipv4 multicast

Syntax

refresh bgp ipv4 multicast { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

View

User view

Default Level

2: Monitor level

Parameters

all: Soft-resets all BGP connections.

ip-address: IP address of an IPv4 MBGP peer.

group-name: Peer group name, a string of 1 to 47 characters.

external: Soft-resets EBGP connections.

internal: Soft-resets IBGP connections.

export: Outbound soft reset.

import: Inbound soft reset.

Description

Use the **refresh bgp ipv4 multicast** command to perform soft reset on specified IPv4 MBGP connections. This method can also refresh the MBGP routing table and apply a new route policy seamlessly.

To perform BGP soft reset, all routers in the network must support route-refresh. If there is a router not supporting the route-refresh function, you need to configure the **peer keep-all-routes** command to save all the routing information of the peer before BGP soft reset.

Examples

Soft-reset all the IPv4 MBGP connections.

```
<Sysname> refresh bgp ipv4 multicast all import
```

reset bgp ipv4 multicast

Syntax

reset bgp ipv4 multicast { **all** | *as-number* | *ip-address* | **group** *group-name* | **external** | **internal** }

View

System view

Default Level

2: Monitor level

Parameters

all: Resets all MBGP connections.

as-number: Resets MBGP connections to peers in the AS.

ip-address: Resets the connection with an IPv4 MBGP peer.

group *group-name*: Resets connections with the specified BGP peer group.

external: Resets all the multicast EBGP connections.

internal: Resets all the multicast IBGP connections.

Description

Use the **reset bgp ipv4 multicast** command to reset specified MBGP connections.

Examples

Reset all the IPv4 MBGP connections.

```
<Sysname> reset bgp ipv4 multicast all
```

reset bgp ipv4 multicast dampening

Syntax

reset bgp ipv4 multicast dampening [*ip-address* [*mask* | *mask-length*]]

View

User view

Default Level

2: Monitor level

Parameters

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation. The default is 255.255.255.255.

mask-length: Mask length, in the range 0 to 32. The default is 32.

Description

Use the **reset bgp ipv4 multicast dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening**, **display bgp multicast routing-table dampened**.

Examples

Clear damping information of route 20.1.0.0/16 and release the suppressed route.

```
<Sysname> reset bgp ipv4 multicast dampening 20.1.0.0 255.255.0.0
```

reset bgp ipv4 multicast flap-info

Syntax

reset bgp ipv4 multicast flap-info [**regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]

View

User view

Default Level

2: Monitor level

Parameters

as-path-regexp: Clears the flap statistics of routes matching the AS path regular expression, which is a string of 1 to 80 case-sensitive characters with spaces included.

as-path-acl-number: Clears the flap statistics for routes matching the AS path ACL, number of which is in the range 1 to 256.

ip-address: Clears the flap statistics of a route.

mask: Mask, in dotted decimal notation. The default is 255.255.255.255.

mask-length: Mask length, in the range 0 to 32. The default is 32.

Description

Use the **reset bgp ipv4 multicast flap-info** command to clear IPv4 MBGP routing flap statistics.

The flap statistics of all the routes will be cleared if no parameter is specified.

Examples

Clear the flap statistics of all IPv4 MBGP routes matching AS path ACL 10.

```
<Sysname> reset bgp ipv4 multicast flap-info as-path-acl 10
```

summary automatic (MBGP family view)

Syntax

summary automatic

undo summary automatic

View

IPv4 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- The default routes and the routes imported with the **network** command cannot be automatically summarized.
- The **summary automatic** command helps IPv4 MBGP limit the number of routes redistributed from IGP.

Examples

In IPv4 MBGP address family view, enable automatic route summarization.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] summary automatic
```

Table of Contents

1 Multicast VPN Configuration Commands

Multicast VPN Configuration Commands

display multicast-domain vpn-instance share-group

Syntax

display multicast-domain vpn-instance *vpn-instance-name* **share-group**

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case sensitive string of up to 31 characters. A VPN instance name must not contain any space.

Description

Use the **display multicast-domain vpn-instance share-group** command to view the share-group information of the specified VPN instance in the MD.

Examples

View the share-group information of VPN instance mvpn in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn share-group
MD local share-group information for VPN-Instance: mvpn
  Share-group: 225.2.2.2
  MTunnel address: 1.1.1.1
```

Table 1-1 display multicast-domain vpn-instance share-group command output description

Field	Description
MD local share-group information for VPN-Instance: mvpn	Share-group information of VPN instance mvpn
Share-group	Share-group address
MTunnel address	MTI address associated with the share-group address

multicast-domain share-group

Syntax

multicast-domain share-group *group-address* **binding mtunnel** *mtunnel-number*

undo multicast-domain share-group

View

VPN instance view

Default Level

2: System level

Parameters

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mtunnel-number: Number of the MTI interface to be created, in the range of 0 to 127.

Description

Use the **multicast-domain share-group** command to configure a share-group address and associate an MTI with the current VPN instance.

Use the **undo multicast-domain share-group** command to restore the system default.

By default, no share-group address is configured and no MTI is associated with a VPN instance.

Note that:

- Do not specify a multicast group address in the public network SSM group range as a share-group address; otherwise a share-MDT cannot be established.
- This command must not be used repeatedly in the same VPN instance view. To configure a new group address and MTI for a VPN instance, you must remove the existing configuration.
- IP multicast routing must be enabled in the VPN instance before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Specify 224.1.1.1 as the share-group address in VPN instance mvpn and associate MTI 0 with the VPN instance.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain share-group 224.1.1.1 binding mtunnel 0
```

Table of Contents

1 IGMP Snooping Configuration Commands

Note

- Configurations made in IGMP Snooping view are effective for all VLANs, while configurations made in VLAN view are effective only for ports belonging to the current VLAN. For a given VLAN, a configuration made in IGMP Snooping view is effective only if the same configuration is not made in VLAN view.
- Configurations made in IGMP Snooping view are effective for all ports; configurations made in Ethernet interface view are effective only for the current port; configurations made in Layer 2 aggregate interface view are effect only for the current interface; configurations made in port group view are effective only for all the ports in the current port group. For a given port, a configuration made in IGMP Snooping view is effective only if the same configuration is not made in Ethernet interface view, Layer 2 aggregate interface view or port group view.
- An IGMP Snooping configuration made on a Layer 2 aggregate interface is independent of the same configuration made on its member ports and is not involved in aggregation calculations. The member ports run the configuration made on the Layer 2 aggregate interface they belong to, and the configuration made on a member port takes effect only when the port is removed from the aggregate group.

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 the IGMP Snooping multicast group information for the specified card. If you do not specify a slot, this command will display the IGMP Snooping multicast group information on the SRPU.

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 unit board: Mask(0x8 3)
    Router port(s):total 1 port.
            Eth2/0/1                (D)
    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 unit board: Mask(0x8 3)
          Host port(s):total 1 port.
            Eth2/0/2                (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port unit board: Mask(0x8 3)
          Host port(s):total 1 port.
            Eth2/0/2
```

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

Field	Description
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. On a distributed device, to get this time value of a non-aggregation port that does not belong to the SRPU, you must specify the number of the slot where the corresponding board resides; this is not required on an aggregation port.
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

drop-unknown (IGMP-Snooping view)

Syntax

drop-unknown

undo drop-unknown

View

IGMP-Snooping view

Default Level

2: System level

Parameters

None

Description

Use the **drop-unknown** command to enable globally the function of dropping unknown multicast data.

Use the **undo drop-unknown** command to disable globally the function of dropping unknown multicast data.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command works only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

Related commands: **igmp-snooping drop-unknown**.

Examples

Globally enable the device to drop unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] drop-unknown
```

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.

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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- 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.

Note

When defining an advanced ACL, include in the **rule** command only the **source** and **destination** keywords without other rule information 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 **group-policy** command to configure a global multicast group filter.

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.

```
<Sysname> system-view
[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 only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

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.

Related commands: **igmp-snooping enable** and **drop-unknown**.

Examples

In VLAN 2, enable IGMP Snooping and the function of dropping unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 interface view, Layer 2 aggregate interface 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.

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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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.

Related commands: **igmp-snooping enable**.

Examples

In VLAN 2, enable IGMP Snooping and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] qui
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 interface view, Layer 2 aggregate interface view, port group view

Default Level

2: System level

Parameters

limit: Maximum number of multicast groups that can be joined on a port, 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 **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 setting depends on the specific product model.

Note that:

- For a switch that supports both IGMP Snooping and IGMP, you can also use the **igmp group-limit** command to limit the number of multicast groups that can be joined on an interface. However, if you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for the VLAN interface of the same VLAN, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of multicast groups only on the VLAN interface..
- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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).

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 an interface, namely a host can join any valid multicast group.

Note that:

- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 on Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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: **igmp-snooping enable , host-aging-time**.

Examples

Enable IGMP Snooping and set the aging time of dynamic member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 interface view, Layer 2 aggregate interface 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) 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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces. The version of IGMP on the simulated host depends on the version of IGMP Snooping running in the VLAN or the version of IGMP running on the VLAN interface.
- 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 interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 2/0/1 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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: **igmp-snooping enable**, **last-member-query-interval**.

Examples

Enable IGMP Snooping and set the interval between IGMP last-member queries to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
```

```
[Sysname-vlan2] igmp-snooping enable
[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: **igmp-snooping enable**, **max-response-time**, **igmp-snooping query-interval**.

Examples

Enable IGMP Snooping and set the maximum response time to IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 interface view, Layer 2 aggregate interface 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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- Be sure to configure the maximum number of multicast groups allowed on a port which cannot be the default value 1000 (refer to igmp-snooping group-limit) before enabling multicast group replacement. Otherwise, the multicast group replacement functionality will not take effect.
- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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: **igmp-snooping enable**; **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable IGMP Snooping and the IGMP Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 enable**, **igmp-snooping querier**, **igmp-snooping max-response-time**, **max-response-time**.

Examples

Enable IGMP Snooping and set the interval between IGMP general queries to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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: **igmp-snooping enable**, **router-aging-time**.

Examples

Enable IGMP Snooping and set the aging time of dynamic router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

View

Ethernet interface 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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

Examples

Enable source port filtering for multicast data on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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.

Related commands: **igmp-snooping enable.**

Examples

In VLAN 2, enable IGMP Snooping and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] qui
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[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 interface view, Layer 2 aggregate interface 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 interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 20/1 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

- If configured in Ethernet interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

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 only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- 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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

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 only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.
- 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 only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

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 both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

Examples

Enable source port filtering for multicast data on interfaces Ethernet 2/0/1 through Ethernet 2/0/4.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port ethernet 2/0/1 to ethernet 2/0/4
```

Table of Contents

1 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 4 multicast-vlan(s)

 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port

 Multicast vlan 200
   subvlan list:
    no subvlan
   port list:
    Eth2/0/1                 Eth2/0/2

 Multicast vlan 300
   subvlan list:
    vlan 3
   port list:
```

```
    Eth2/0/3                Eth2/0/4

 Multicast vlan 400
   subvlan list:
    no subvlan
   port list:
    no port
```

Table 1-1 display multicast-vlan command output description

Field	Description
Total 4 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.
- The multicast VLAN feature cannot be enabled on a device with IP multicast routing enabled.
- 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: **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*; **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 interfaces can be configured as multicast VLAN ports: Ethernet, or Layer 2 aggregate interfaces.

Examples

Assign ports Ethernet 2/0/1 through Ethernet 2/0/5 to multicast VLAN 100.

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

```
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] port ethernet 2/0/1 to ethernet 2/0/5
```

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 the system-defined limit (an S7900E series Ethernet switch supports up to five multicast VLANs, and supports up to 4000 sub-VLANs for each multicast VLAN. The total number of sub-VLANs for all multicast VLANs on the switch cannot exceed 4000.).

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
```

Table of Contents

1 IPv6 Multicast Routing and Forwarding Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running an IP multicast routing protocol.

IPv6 Multicast Routing and Forwarding Configuration Commands

display multicast ipv6 boundary

Syntax

display multicast ipv6 boundary [*ipv6-group-address* [*prefix-length*]] [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of an IPv6 multicast group address, in the range of 8 to 128. The system default is 128.

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

Description

Use the **display multicast ipv6 boundary** command to display the IPv6 multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast ipv6 boundary**.

Examples

Display the IPv6 multicast boundary information configured on all interfaces.

```
<Sysname> display multicast ipv6 boundary
```

```
IPv6 multicast boundary information
 Boundary            Interface
 FF03::/16           Vlan1
 FF09::/16           Vlan2
```

Table 1-1 display multicast ipv6 boundary command output description

Field	Description
IPv6 multicast boundary information	IPv6 multicast boundary
Boundary	IPv6 multicast group corresponding to the IPv6 multicast boundary
Interface	Boundary interface corresponding to the IPv6 multicast boundary

display multicast ipv6 forwarding-table

Syntax

display multicast ipv6 forwarding-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-number*] * [**port-info**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-source-address: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays the forwarding entries whose incoming interface is the specified one.

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

register: Represents a registered interface.

outgoing-interface: Displays the forwarding entries whose outgoing interface is the specified one.

exclude: Displays the forwarding entries whose outgoing interface list excludes the specified interface.

include: Displays the forwarding entries whose outgoing interface list includes the specified interface.

match: Displays the forwarding entries whose outgoing interface list includes and includes only the specified interface.

statistics: Specifies to display the statistics information of the IPv6 multicast forwarding table.

slot *slot-number*: Specifies the slot number of an interface card. If you do not provide this option, the multicast forwarding table information of the main processing board will be displayed.

port-info: Displays Layer 2 port information.

Description

Use the **display multicast ipv6 forwarding-table** command to display information of the IPv6 multicast forwarding table.

IPv6 multicast forwarding tables are used to guide multicast forwarding. You can view the state of IPv6 multicast traffic forwarding by checking the IPv6 multicast forwarding table.

Related commands: **multicast ipv6 forwarding-table downstream-limit**, **multicast ipv6 forwarding-table route-limit**, **display multicast ipv6 routing-table**.

Examples

Display information of the IPv6 multicast forwarding table.

```
<Sysname> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 1 entry

Total 1 entry matched

00001. (2000:5::1:1000, FF1E::1234)
     MID: 0, Flags: 0x0:0
     Uptime: 04:04:37, Timeout in: 00:03:26
     Incoming interface: Vlan-interface1
     List of 1 outgoing interfaces:
       1: Vlan-interface2
     Matched 146754 packets(10272780 bytes), Wrong If 0 packets
     Forwarded 139571 packets(9769970 bytes)
```

Table 1-2 display multicast ipv6 forwarding-table command output description

Field	Description
IPv6 Multicast Forwarding Table	IPv6 multicast forwarding table
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast forwarding table
Total 1 entry matched	Total number of matched (S, G) entries in the IPv6 multicast forwarding table
00001	Sequence number of the (S, G) entry
(2000:5::1:1000, FF1E::1234)	An (S, G) entry in the IPv6 multicast forwarding table
MID	MID of the (S, G). Each (S, G) entry has a unique MID.
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of the (S, G) entry. For the values and meanings of this field, see Table 1-3.

Field	Description
Uptime	Length of time for which the (S, G) entry has been up
Timeout in	Length of time in which the (S, G) entry will time out
Incoming interface	Incoming interface of the (S, G) entry
List of 1 outgoing interfaces: 1: Vlan-interface2	Outgoing interface list: Interface number: interface type and number
Matched 146754 packets(10272780 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors
Forwarded 139571 packets(9769970 bytes)	(S, G) forwarded IPv6 multicast packets (bytes)

Table 1-3 Values and meanings of the Flags field

Value	Meaning
0x00000001	Indicates that a register-stop message needs to be sent.
0x00000002	Indicates whether the IPv6 multicast source corresponding to the (S, G) entry is active.
0x00000004	Indicates a null forwarding entry.
0x00000008	Indicates whether the RP is a border router in an IPv6 PIM domain.
0x00000010	Indicates a register outgoing interface is available.
0x00000400	Indicates an (S, G) entry to be deleted.
0x00008000	Indicates that the (S, G) entry is in smoothening process after active/standby switchover.
0x00010000	Indicates that the (S, G) entry has been updated during the smoothening process.
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and need to be deleted before a new entry is added.
0x00100000	Indicates that the (S, G) entry was added successfully

display multicast ipv6 routing-table

Syntax

display multicast ipv6 routing-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-source-address: Multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of a multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays routing entries whose incoming interface is the specified one.

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

register: Represents a registered interface.

outgoing-interface: Displays routing entries of which the outgoing interface is the specified one.

exclude: Displays routing entries whose outgoing interface list excludes the specified interface.

include: Displays routing entries whose outgoing interface list includes the specified interface.

match: Displays routing entries whose outgoing interface list includes only the specified interface.

Description

Use the **display multicast ipv6 routing-table** command to display the information of an IPv6 multicast routing table.

IPv6 multicast routing tables are the basis of IPv6 multicast forwarding. You can view the establishment state of an (S, G) entry by checking the IPv6 multicast routing table.

Related commands: **display multicast ipv6 forwarding-table**.

Examples

Display the information of an IPv6 multicast routing table.

```
<Sysname> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (2001::2, FFE3::101)
       Uptime: 00:00:14
       Upstream Interface: Vlan-interface1
       List of 1 downstream interface
           1:  Vlan-interface2
```

Table 1-4 display multicast ipv6 routing-table command output description

Field	Description
IPv6 multicast routing table	IPv6 multicast routing table
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast routing table
00001	Sequence number of the (S, G) entry
(2001::2, FFE3::101)	An (S, G) entry in the IPv6 multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up.

Field	Description
Upstream interface	Upstream interface of the (S, G) entry. Multicast packets should arrive through this interface.
List of 2 downstream interfaces	Downstream interface list. These interfaces need to forward multicast packets.

display multicast ipv6 rpf-info

Syntax

display multicast ipv6 rpf-info *ipv6-source-address* [*ipv6-group-address*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-source-address: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number from 0 to F.

Description

Use the **display multicast ipv6 rpf-info** command to display RPF information of an IPv6 multicast source.

Related commands: **display multicast ipv6 routing-table**, **display multicast ipv6 forwarding-table**.

Examples

Display all RPF information of the multicast source with an IPv6 address 2001::101.

```
<Sysname> display multicast ipv6 rpf-info 2001::101
 RPF information about source 2001::101:
     RPF interface: Vlan-interface1, RPF neighbor: 2002::201
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 1-5 display multicast ipv6 rpf-info command output description

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101
RPF interface	Indicates the interface type and number of the RPF interface
RPF neighbor	Indicate the IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Referenced route and prefix length

Field	Description
Referenced route type	Type of the referenced route, which can be any of the following: • igp: IPv6 unicast route (IGB). • egp: IPv6 unicast (EGP). • unicast (direct): IPv6 unicast route (directly connected). • unicast: other IPv6 unicast route (such as IPv6 unicast static route). • mbgp: IPv6 MBGP route.
Route selection rule	RPF route selection rule: An RPF route can be selected by the priority of the routing protocol or by the longest match of the destination address in the routing table.
Load splitting rule	Load sharing rule

multicast ipv6 boundary

Syntax

multicast ipv6 boundary *ipv6-group-address prefix-length*

undo multicast ipv6 boundary { *ipv6-group-address prefix-length* | **all** }

View

Interface view

Default Level

2: System level

Parameters

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of an IPv6 multicast group address, in the range of 8 to 128.

all: Deletes all IPv6 multicast boundaries configured on the interface.

Description

Use the **multicast ipv6 boundary** command to configure an IPv6 multicast forwarding boundary.

Use the **undo multicast ipv6 boundary** command to delete the specified IPv6 multicast forwarding boundary or all IPv6 multicast forwarding boundaries.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple IPv6 multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and that B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on

the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast ipv6 boundary**.

Examples

Configure VLAN-interface 100 to be the forwarding boundary of the IPv6 multicast group FF03::101/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast ipv6 boundary ff03::101 16
```

multicast ipv6 forwarding-table downstream-limit

Syntax

multicast ipv6 forwarding-table downstream-limit *limit*

undo multicast ipv6 forwarding-table downstream-limit

View

System view

Default Level

2: System level

Parameters

limit: Maximum number of downstream nodes (namely the maximum number of outgoing interfaces) for a single entry in the IPv6 multicast forwarding table. The value ranges 0 to 128.

Description

Use the **multicast ipv6 forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table is the maximum number allowed by the system, namely 128.

Examples

Set the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table downstream-limit 120
```

multicast ipv6 forwarding-table route-limit

Syntax

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

View

System view

Default Level

2: System level

Parameters

limit: Maximum number of entries in the IPv6 multicast forwarding table. The value ranges from 0 to 512.

Description

Use the **multicast ipv6 forwarding-table route-limit** command to configure the maximum number of entries in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table route-limit** command to restore the system default.

By default, the maximum number of entries in the IPv6 multicast forwarding table is the maximum number allowed by the system, namely 512.

Related commands: **display multicast ipv6 forwarding-table**.

Examples

Set the maximum number of entries in the IPv6 multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table route-limit 200
```

multicast ipv6 load-splitting

Syntax

multicast ipv6 load-splitting {**source** | **source-group** }

undo multicast ipv6 load-splitting

View

System view

Default Level

2: System level

Parameters

source: Specifies to implement IPv6 multicast load splitting on a per-source basis.

source-group: Specifies to implement IPv6 multicast load splitting on a per-source and per-group basis.

Description

Use the **multicast load-splitting** command to enable load splitting of IPv6 multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of IPv6 multicast traffic.

By default, load splitting of IPv6 multicast traffic is disabled.

Examples

Enable load splitting of IPv6 multicast traffic on a per-source basis.

```
<Sysname> system-view
[Sysname] multicast ipv6 load-splitting source
```

multicast ipv6 longest-match

Syntax

multicast ipv6 longest-match

undo multicast ipv6 longest-match

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **multicast ipv6 longest-match** command to configure RPF route selection based on the longest match principle, namely to select the route with the longest prefix as the RPF route.

Use the **undo multicast ipv6 longest-match** command to restore the default.

By default, the route with the highest priority is selected as the RPF route.

Examples

Configure RPF route selection based on the longest match.

```
<Sysname> system-view
[Sysname] multicast ipv6 longest-match
```

multicast ipv6 routing-enable

Syntax

multicast ipv6 routing-enable

undo multicast ipv6 routing-enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **multicast ipv6 routing-enable** command to enable IPv6 multicast routing.

Use the **undo multicast ipv6 routing-enable** command to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

Note that:

- You must enable IPv6 multicast routing before you can carry out other Layer 3 IPv6 multicast commands.
- The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Examples

Enable IPv6 multicast routing.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
```

reset multicast ipv6 forwarding-table

Syntax

reset multicast ipv6 forwarding-table { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View

User view

Default Level

2: System level

Parameters

ipv6-source-address: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Prefix length of an IPv6 multicast group or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Specifies to clear IPv6 multicast forwarding entries of which the incoming interface is the specified one.

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

register: Specifies the register interface.

all: Clears all forwarding entries from the IPv6 multicast forwarding table.

Description

Use the **reset multicast ipv6 forwarding-table** command to clear forwarding entries from the IPv6 multicast forwarding table.

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry is also deleted from the IPv6 multicast routing table.

Related commands: **reset multicast IPv6 routing-table**, **display multicast ipv6 routing-table**, **display multicast ipv6 forwarding-table**.

Examples

Clear the IPv6 multicast forwarding entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast forwarding table.

```
<Sysname> reset multicast ipv6 forwarding-table ff03::101
```

reset multicast ipv6 routing-table

Syntax

reset multicast ipv6 routing-table { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View

User view

Default Level

2: System level

Parameters

ipv6-source-address: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Clears IPv6 multicast routing entries of which the incoming interface is the specified one.

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

register: Specifies a register interface.

all: Clears all routing entries from the IPv6 multicast routing table.

Description

Use the **reset multicast ipv6 routing-table** command to clear IPv6 routing entries from the IPv6 multicast routing table.

When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry is also deleted from the IPv6 multicast forwarding table.

Related commands: **reset multicast ipv6 forwarding-table**, **display multicast ipv6 forwarding-table**, **display multicast ipv6 routing-table**.

Examples

Clear the routing entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast routing table.

```
<Sysname> reset multicast ipv6 routing-table ff03::101
```

Table of Contents

1 MLD Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running MLD.

MLD Configuration Commands

display mld group

Syntax

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: MLD multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

interface *interface-type interface-number*: Displays the information of MLD multicast groups on the specified interface.

static: Displays the information of statically joined MLD multicast groups.

verbose: Displays detailed information of MLD multicast groups.

Description

Use the **display mld group** command to view information of MLD multicast groups.

Note that:

- If you do not specify an IPv6 mutlicast group address, this command will display the MLD information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the MLD multicast group information on all the interfaces.
- If you do not specify the **static** keyword, the information of only dynamically joined MLD groups will be displayed.

Examples

View the detailed information of dynamically joined MLD multicast groups on all interfaces.

```
<Sysname> display mld group verbose
Interface group report information
Vlan-interface1(FE80::101)
  Total 1 MLD Groups reported
   Group: FF03::101
     Uptime: 00:01:46
     Expires: 00:01:30
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: include
     Version1-host-present-timer-expiry: off
```

Table 1-1 display mld group command output description

Field	Description
Interface group report information	MLD multicast group information on the interface
Total 1 MLD Groups reported	One MLD multicast group was reported.
Group	IPv6 multicast group address
Uptime	Length of time since the IPV6 multicast group was joined
Expires	Remaining time of the IPv6 multicast group , where “off" means that the multicast group never times out
Last reporter	IPv6 address of the host that last reported membership for this group
Last-listener-query-counter	Number of MLD multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer , where “off" means that the timer never times out
Group mode	Filtering mode of multicast sources
Version1-host-present-timer-expiry	Remaining time of the MLDv1 host present timer , where “off" means that the timer never times out

display mld group port-info

Syntax

display mld group port-info [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command will display the Layer 2 port information of MLD multicast groups in all VLANs.

slot *slot-number*: Displays the Layer 2 port information about MLD multicast groups on the specified card. If you do not specify a slot number, this command will display the Layer 2 port information about MLD multicast groups on the main processing unit.

verbose: Displays the detailed information about Layer 2 ports of MLD multicast groups.

Description

Use the **display mld group port-info** command to view Layer 2 port information of MLD multicast groups.

Examples

View detailed Layer 2 port information of MLD multicast groups.

```
<Sysname> display mld group port-info 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.
            Vlan1                (D) ( 00:01:30 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF03::101
        (FE80::1, FF03::101):
          Attribute:    Host Port
          Host port(s):total 1 port.
            Vlan2                (D) ( 00:03:23 )
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            Vlan2
```

Table 1-2 display mld group port-info 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 flag: D stands for dynamic port, S for static port, and C for port copied from a (*, G) entry to an (S, G) entry.

Field	Description
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flag: R stands for real egress sub-VLAN under the current entry, and 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 dynamic member port or router port aging timer. On a distributed device, to get this time value of a non-aggregation port on a board other than the main processing unit, you must specify the number of the slot where the corresponding board resides by using **slot** *slot-number*. This is not required for an aggregation port.
IP group address	Address of an IPv6 multicast group
MAC group address	Address of a MAC multicast group
Attribute	Attribute of an IPv6 multicast group
Host port(s)	Number of member ports

display mld interface

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command will display the information of all interfaces running MLD.

verbose: Displays detailed MLD configuration and operation information.

Description

Use the **display mld interface** command to view MLD configuration and operation information on the specified interface or all MLD-enabled interfaces.

Examples

View the detailed MLD configuration and operation information on Vlan-interface 1.

```
<Sysname> display mld interface vlan-interface 1 verbose
 Vlan-interface1(FE80::200:AFF:FE01:101):
   MLD is enabled
   Current MLD version is 2
   Value of query interval for MLD(in seconds): 125
```

```
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Value of last listener query interval(in seconds): 1
  Value of startup query interval(in seconds): 31
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:23
  Querier for MLD: FE80::200:AFF:FE01:101 (this router)
  MLD activity: 1 joins, 0 leaves
  Multicast ipv6 routing on this interface: enabled
  Robustness: 2
  Require-router-alert: disabled
  Fast-leave: disabled
  Ssm-mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
Total 1 MLD Group reported
```

Table 1-3 display mld group port-info command output description

Field	Description
Ethernet1/1(FE80::200:AFF:FE01:101)	Interface name (IPv6 link-local address)
Current MLD version	MLD version running on the interface
MLD group policy	MLD group policy
Value of query interval for MLD (in seconds)	MLD query interval, in seconds
Value of other querier present interval for MLD (in seconds)	MLD other querier present interval, in seconds
Value of maximum query response time for MLD (in seconds)	Maximum response delay for general query messages (in seconds)
Value of last listener query interval (in seconds)	MLD last listener query interval, in seconds
Value of startup query interval(in seconds)	MLD startup query interval, in seconds
Value of startup query count	Number of MLD general queries sent on startup
General query timer expiry	Remaining time of the MLD general query timer , where “off" means that the timer never times out
Querier for MLD	IPv6 link-local address of the MLD querier
MLD activity	MLD activity statistics (number of join and done messages)
Robustness	MLD querier robustness variable
Require-router-alert	Dropping MLD messages without Router-Alert (enabled/disabled)
Fast-leave	MLD fast leave processing status (enabled/disabled)
Ssm-mapping	MLD SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of MLD startup query timer , where “off" means that the timer never times out

Field	Description
Other-querier-present-timer-expiry	Remaining time of MLD other querier present timer , where “off" means that the timer never times out
Total 1 MLD Group reported	Total number of MLD groups the interface has dynamically joined

display mld routing-table

Syntax

display mld routing-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*]] *

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-source-address: Specifies a multicast source by its IPv6 address.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

prefix-length: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description

Use the **display mld routing-table** command to view the information of the MLD routing table.

Examples

View the information of the MLD routing table.

```
<Sysname> display mld routing-table
Routing table
 Total 1 entry

 00001. (*, FF1E::101)
       List of 1 downstream interface
        Vlan-interface1 (FE80::200:5EFF:FE71:3800),
                   Protocol: MLD
```

Table 1-4 display mld routing-table command output description

Field	Description
Routing table	MLD routing table
00001	Sequence number of this (*, G) entry

Field	Description
(*, FF1E::101)	An (*, G) entry in the MLD routing table
List of 1 downstream interface	List of downstream interfaces: namely the interfaces to which multicast data for this group will be forwarded
Protocol	Protocol type

display mld ssm-mapping

Syntax

display mld ssm-mapping *ipv6-group-address*

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

Description

Use the **display mld ssm-mapping** command to view the configured MLD SSM mappings for the specified IPv6 multicast group.

Related commands: **ssm-mapping**.

Examples

View the MLD SSM mappings for multicast group FF1E::101.

```
<Sysname> display mld ssm-mapping ff1e::101
 Group: FF1E::101
 Source list:
        1::1
        1::2
        10::1
        100::10
```

Table 1-5 display mld ssm-mapping command output description

Field	Description
Group	IPv6 multicast group address
Source list	List of IPv6 multicast source addresses

display mld ssm-mapping group

Syntax

display mld ssm-mapping group [*ipv6-group-address* | **interface** *interface-type interface-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: Specifies a multicast group by its IPv6 address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

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

verbose: Displays the detailed multicast group information created based on the configured MLD SSM mappings.

Description

Use the **display mld ssm-mapping group** command to view the multicast group information created based on the configured MLD SSM mappings.

Note that:

- If you do not specify an IPv6 multicast group, this command will display the information of all IPv6 multicast groups created based on the configured MLD SSM mappings.
- If you do not specify an interface, this command will display the multicast group information created based on the configured MLD SSM mappings on all interfaces.

Examples

View the detailed information of IPv6 multicast group FF3E::101 created based on the configured MLD SSM mappings on all interfaces.

```
<Sysname> display mld ssm-mapping group ff3e::101 verbose
Interface group report information
 Vlan-interface1(FE80::101):
  Total 1 MLD SSM-mapping Group reported
   Group: FF3E::101
     Uptime: 00:01:46
     Expires: off
     Last reporter: FE80::10
     Group mode: include
     Source list(Total 1 source):
       Source: 30::1
          Uptime: 00:01:46
          Expires: 00:02:34
          Last-listener-query-counter: 0
```

```
Last-listener-query-timer-expiry: off
```

Table 1-6 display mld ssm-mapping group command output description

Field	Description
Interface group report information	IPv6 multicast group information created based on MLD SSM mappings on the interface
Total 1 MLD SSM-mapping Group reported	One MLD SSM mapping multicast group was reported.
Group	IPv6 multicast group address
Uptime	Length of time since the IPv6 multicast group was reported
Expires	Remaining time of the IPv6 multicast group , where “off” means that the group never times out
Last reporter	IPv6 address of the host that last reported membership for this group
Group mode	IPv6 multicast sources filter mode
Source list(Total 1 source)	IPv6 multicast source list (one IPv6 multicast source)
Source	IPv6 multicast source address
Last-listener-query-counter	Number of MLD multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer , where “off” means that the timer never expires

last-listener-query-interval (MLD view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD view

Default Level

2: System level

Parameters

interval: MLD last listener query interval in 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.

Related commands: **mld last-listener-query-interval**, **robust-count**, **display mld interface**.

Examples

Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-interval 3
```

max-response-time (MLD view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD view

Default Level

2: System level

Parameters

interval: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description

Use the **max-response-time** command to configure the maximum response delay for MLD general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response delay for MLD general queries is 10 seconds.

Related commands: **mld max-response-time**, **timer other-querier-present**, **display mld interface**.

Examples

Set the maximum response delay for MLD general queries to 8 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 8
```

mld

Syntax

mld

undo mld

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **mld** command to enter MLD view.

Use the **undo mld** command to remove the configurations made in MLD view.

Note that this command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **mld enable**; **multicast ipv6 routing-enable** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume.*

Examples

Enable IPv6 multicast routing and enter MLD view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] mld
[Sysname-mld]
```

mld enable

Syntax

mld enable

undo mld enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **mld enable** command to enable MLD on the current interface.

Use the **undo mld enable** command to disable MLD on the current interface.

By default, MLD is disabled on the current interface.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- Other MLD configurations performed on the interface can take effect only after MLD is enabled on the interface.

Related commands: **mld**; **multicast ipv6 routing-table** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IPv6 multicast routing and enable MLD on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld enable
```

mld group-policy

Syntax

mld group-policy *acl6-number* [*version-number*]

undo mld group-policy

View

Interface view

Default Level

2: System level

Parameters

acl6-number: Number of a basic or advanced IPv6 ACL, in the range of 2000 to 3999. The 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 a IPv6 multicast source address of 0::0.

version-number: MLD version number, 1 or 2. If you do not specify an MLD version, the configured group filter will be effective for MLD reports of both version 1 and version 2.

Description

Use the **mld group-policy** command to configure an IPv6 multicast group filter on the current interface to limit access to the IPv6 multicast group.

Use the **undo mld group-policy** command to remove the configured IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured by default, that is, a host can join any valid IPv6 multicast group.

Examples

Configure an IPv6 ACL so that hosts on the subnet attached to Vlan-interface1 can join the IPv6 multicast group FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2005
[Sysname-acl6-basic-2005] rule permit source ff03::101 128
[Sysname-acl6-basic-2005] quit
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] mld group-policy 2005
```

mld last-listener-query-interval

Syntax

mld last-listener-query-interval *interval*

undo mld last-listener-query-interval

View

Interface view

Default Level

2: System level

Parameters

interval: MLD last listener query interval in seconds, in the range of 1 to 5.

Description

Use the **mld last-listener-query-interval** command to configure the MLD last listener query interval on the current interface.

Use the **undo mld last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

Related commands: **last-listener-query-interval**, **mld robust-count**, **display mld interface**.

Examples

Set the MLD last listener query interval to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-interval 3
```

mld max-response-time

Syntax

mld max-response-time *interval*

undo mld max-response-time

View

Interface view

Default Level

2: System level

Parameters

interval: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description

Use the **mld max-response-time** command to configure the maximum response delay for MLD general query messages on the interface.

Use the **undo mld max-response-time** command to restore the default configuration.

By default, the maximum response delay for MLD general query messages is 10 seconds.

The maximum response delay determines the time which the device takes to detect directly attached group members in the LAN.

Related commands: **max-response-time**, **mld timer other-querier-present**, **display mld interface**.

Examples

Set the maximum response delay for MLD general query messages to 8 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld max-response-time 8
```

mld require-router-alert

Syntax

mld require-router-alert

undo mld require-router-alert

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **mld require-router-alert** command to configure the interface to discard MLD messages without the Router-Alert option.

Use the **undo mld require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **require-router-alert**, **mld send-router-alert**.

Examples

Configure VLAN-interface 100 to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld require-router-alert
```

mld robust-count

Syntax

mld robust-count *robust-value*

undo mld robust-count

View

Interface view

Default Level

2: System level

Parameters

robust-value: MLD querier robustness variable, with an effective range of 2 to 5.

Description

Use the **mld robust-count** command to configure the MLD querier robustness variable on the current interface.

Use the **undo mld robust-count** command to restore the system default.

By default, the MLD querier robustness variable is 2.

Related commands: **robust-count**, **mld timer query**, **mld last-listener-query-interval**, **mld timer other-querier-present**, **display mld interface**.

Examples

Set the MLD querier robustness variable to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld robust-count 3
```

mld send-router-alert

Syntax

mld send-router-alert

undo mld send-router-alert

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **mld send-router-alert** command to enable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

Use the **undo mld send-router-alert** command to disable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

By default, MLD messages carry the Router-Alert option.

Related commands: **send-router-alert**, **mld require-router-alert**.

Examples

Disable insertion of the Router-Alert option into MLD messages to be sent from VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo mld send-router-alert
```

mld ssm-mapping enable

Syntax

mld ssm-mapping enable

undo mld ssm-mapping enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **mld ssm-mapping enable** command to enable the MLD SSM mapping feature on the current interface.

Use the **undo mld ssm-mapping enable** command to disable the MLD SSM mapping feature on the current interface.

By default, the MLD SSM mapping feature is disabled on all interfaces.

Examples

Enable the MLD SSM mapping feature on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld ssm-mapping enable
```

mld startup-query-count

Syntax

mld startup-query-count *value*

undo mld startup-query-count

View

Interface view

Default Level

2: System level

Parameters

value: Startup query count, namely, the number of queries the MLD querier sends on startup, with an effective range of 2 to 5.

Description

Use the **mld startup-query-count** command to configure the startup query count on the current interface.

Use the **undo mld startup-query-count** command to restore the system default.

By default, the startup query count is set to the MLD querier robustness variable.

 **Note**

By default, the MLD querier robustness variable is 2, so the startup query count is also 2.

Related commands: **startup-query-count**, **mld robust-count**.

Examples

Set the startup query count to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-count 3
```

mld startup-query-interval

Syntax

mld startup-query-interval *interval*

undo mld startup-query-interval

View

Interface view

Default Level

2: System level

Parameters

interval: Startup query interval in seconds, namely, the interval between general queries the MLD querier sends on startup, with an effective range of 1 to 18000.

Description

Use the **mld startup-query-interval** command to configure the startup query interval on the current interface.

Use the **undo mld startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the MLD query interval.

Note

By default, the MLD query interval is 125 seconds, so the startup query interval = 125 / 4 = 31.25 (seconds).

Related commands: **startup-query-interval**, **mld timer query**.

Examples

Set the startup query interval to 5 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-interval 5
```

mld static-group

Syntax

mld static-group *ipv6-group-address* [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**source** *ipv6-source-address*] }

View

Interface view

Default Level

2: System level

Parameters

all: Removes all static IPv6 multicast groups that the current interface has joined.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. .

ipv6-source-address: IPv6 address of the specified multicast source.

Description

Use the **mld static-group** command to configure the current interface to be a statically-connected member of the specified IPv6 multicast group or IPv6 multicast source and group.

Use the **undo mld static-group** command to remove the configuration.

By default, an interface is not a statically-connected member of any IPv6 multicast group or IPv6 multicast source and group.

If the IPv6 multicast address is in the SSM multicast address range, you must specify an IPv6 multicast source address at the same time; otherwise MLD routing table entries cannot be established. There is no such a restriction if the specified IPv6 multicast group address is not in the SSM multicast address range.

Examples

Configure Vlan-interface1 to be a statically-connected member of the IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Ethernet1/1] mld static-group ff03::101
```

Configure Vlan-interface1 as a static member to forward multicast data of the multicast source 2001::101 to the multicast group FF3E::202.

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] mld static-group ff3e::202 source 2001::101
```

mld timer other-querier-present

Syntax

mld timer other-querier-present *interval*

undo mld timer other-querier-present

View

Interface view

Default Level

2: System level

Parameters

interval: MLD other querier present interval in seconds, in the range of 60 to 300.

Description

Use the **mld timer other-querier-present** command to configure the MLD other querier present interval on the current interface.

Use the **undo mld timer other-querier-present** command to restore the system default.

By default, MLD other querier present interval = [MLD query interval] times [MLD querier robustness variable] plus [maximum response delay for MLD general queries] divided by two.

Note

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the MLD other querier present interval is 125 x 2 + 10 / 2 = 255 (seconds).

Related commands: **timer other-querier-present**, **mld timer query**, **mld robust-count**, **mld max-response-time**, **display mld interface**.

Examples

Set the MLD other querier present interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface100
[Sysname-Vlan-interface100] mld timer other-querier-present 200
```

mld timer query

Syntax

mld timer query *interval*

undo mld timer query

View

Interface view

Default Level

2: System level

Parameters

interval: MLD query interval, namely the amount of time in seconds between MLD general query messages, in the range of 1 to 18,000.

Description

Use the **mld timer query** command to configure the MLD query interval on the current interface.

Use the **undo mld timer query** command to restore the system default.

By default, the MLD query interval is 125 seconds.

Related commands: **timer query**, **mld timer other-querier-present**, **display mld interface**.

Examples

Set the MLD query interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld timer query 200
```

mld version

Syntax

mld version *version-number*

undo mld version

View

Interface view

Default Level

2: System level

Parameters

version-number: MLD version, 1 or 2.

Description

Use the **mld version** command to configure the MLD version on the current interface.

Use the **undo mld version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related commands: **version**.

Examples

Set the MLD version to MLDv2 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld version 2
```

require-router-alert (MLD view)

Syntax

require-router-alert

undo require-router-alert

View

MLD view

Default Level

2: System level

Parameters

None

Description

Use the **require-router-alert** command to globally configure the device to discard MLD messages without the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **mld require-router-alert**, **send-router-alert**.

Examples

Globally configure the device to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] require-router-alert
```

reset mld group

Syntax

reset mld group { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

View

User view

Default Level

2: System level

Parameters

all: The first **all** specifies to clear MLD multicast group information on all interfaces, while the second **all** specifies to clear the information of all MLD multicast groups.

interface *interface-type interface-number*: Clears the MLD multicast group information on the specified interface.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: IPv6 multicast source address.

prefix-length: Prefix length of the specified multicast source or multicast group. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description

Use the **reset mld group** command to clear MLD multicast group information.

Note that this command cannot clear MLD multicast group information of static joins.

Related commands: **display mld group**.

Examples

Clear all MLD multicast group information on all interfaces.

```
<Sysname> reset mld group all
```

Clear all MLD multicast group information for VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 all
```

Clear the information about MLD multicast group FF03::101:10 on VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 ff03::101:10
```

reset mld group port-info

Syntax

reset mld group port-info { **all** | *ipv6-group-address* } [**vlan** *vlan-id*]

View

User view

Default Level

2: System level

Parameters

all: Clears Layer 2 port information of all the MLD multicast groups.

Ipv6-group-address: Clears Layer 2 port information of the specified MLD multicast group. The effective range of *group-address* is FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

vlan-id: Clear Layer 2 port information of MLD multicast groups in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

Description

Use the **reset mld group port-info** command to clear Layer 2 port information of MLD multicast groups.

Note that:

- Layer 2 ports for MLD multicast groups include member ports and router ports.
- This command cannot clear Layer 2 port information about MLD multicast groups of static joins.

Related commands: **display mld group port-info**.

Examples

Clear Layer 2 port information of all MLD multicast groups in all VLANs.

```
<Sysname> reset mld group port-info all
```

Clear Layer 2 port information of all MLD multicast groups in VLAN 100.

```
<Sysname> reset mld group port-info all vlan 100
```

Clear Layer 2 port information about multicast group FF03::101:10 in VLAN 100.

```
<Sysname> reset mld group port-info ff03::101:10 vlan 100
```

reset mld ssm-mapping group

Syntax

reset mld ssm-mapping group { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

View

User view

Default Level

2: System level

Parameters

all: The first **all** specifies to clear IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces, while the second **all** specifies to clear all IPv6 multicast group information created based on the configured MLD SSM mappings..

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

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: Specifies a multicast source by its IPv6 address.

prefix-length: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description

Use the **reset mld ssm-mapping group** command to clear IPv6 multicast group information created based on the configured MLD SSM mappings.

Related commands: **display mld ssm-mapping group**.

Examples

Clear all IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces.

```
<Sysname> reset mld ssm-mapping group all
```

robust-count (MLD view)

Syntax

robust-count *robust-value*

undo robust-count

View

MLD view

Default Level

2: System level

Parameters

robust-value: MLD querier robustness variable, with an effective range of 2 to 5.

Description

Use the **robust-count** command to configure the MLD querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the MLD querier robustness variable is 2.

Related commands: **mld robust-count**, **last-listener-query-interval**, **timer other-querier-present**, **display mld interface**.

Examples

Set the MLD querier robustness variable to 3 globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 3
```

send-router-alert (MLD view)

Syntax

send-router-alert

undo send-router-alert

View

MLD view

Default Level

2: System level

Parameters

None

Description

Use the **send-router-alert** command to globally enable the insertion of the Router-Alert option into MLD messages to be sent.

Use the **undo send-router-alert** command to globally disable the insertion of the Router-Alert option into MLD messages to be sent.

By default, MLD messages carry the Router-Alert option.

Related commands: **mld send-router-alert**, **require-router-alert**.

Examples

Globally disable insertion of the Router-Alert option into MLD messages to be sent.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] undo send-router-alert
```

ssm-mapping (MLD view)

Syntax

ssm-mapping *ipv6-group-address prefix-length ipv6-source-address*

undo ssm-mapping { *ipv6-group-address prefix-length ipv6-source-address* | **all** }

View

MLD view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

prefix-length: Prefix length of the IPv6 multicast group address, in the range of 8 to 128.

ipv6-source-address: Specifies a multicast source by its IPv6 address.

all: Removes all MLD SSM mappings.

Description

Use the **ssm-mapping** command to configure an MLD SSM mapping.

Use the **undo ssm-mapping** command to remove one or all MLD SSM mappings.

By default, no MLD SSM mappings are configured.

Related commands: **mld ssm-mapping enable**, **display mld ssm-mapping**.

Examples

Configure an MLD SSM mapping for multicast group FF1E::101/64 and multicast source 1::1.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] ssm-mapping ff1e::101 64 1::1
```

startup-query-count (MLD view)

Syntax

startup-query-count *value*

undo startup-query-count

View

MLD view

Default Level

2: System level

Parameters

value: Startup query count, namely, the number of queries the MLD querier sends on startup, with an effective range of 2 to 5.

Description

Use the **startup-query-count** command to configure the startup query count globally.

Use the **undo startup-query-count** command to restore the system default.

By default, the startup query count is set to the MLD querier robustness variable.

Note

By default, the MLD querier robustness variable is 2, so the startup query count is also 2.

Related commands: **mld startup-query-count**, **robust-count**.

Examples

Set the startup query count to 3 globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] startup-query-count 3
```

startup-query-interval (MLD view)

Syntax

startup-query-interval *interval*

undo startup-query-interval

View

MLD view

Default Level

2: System level

Parameters

interval: Startup query interval in seconds, namely, the interval between general queries the MLD querier sends on startup, with an effective range of 1 to 18000.

Description

Use the **startup-query-interval** command to configure the startup query interval globally.

Use the **undo startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the “MLD query interval”.

Note

By default, the MLD query interval is 125 seconds, so the startup query interval = 125 / 4 = 31.25 (seconds).

Related commands: **mld startup-query-interval**, **timer query**.

Examples

Set the startup query interval to 5 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] startup-query-interval 5
```

timer other-querier-present (MLD view)

Syntax

timer other-querier-present *interval*

undo timer other-querier-present

View

MLD view

Default Level

2: System level

Parameters

interval: MLD other querier present interval in seconds, in the range of 60 to 300.

Description

Use the **timer other-querier-present** command to configure the MLD other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the default configuration.

By default, MLD other querier present interval = [MLD query interval] times [MLD querier robustness variable] plus [maximum response delay for MLD general queries] divided by two.

 **Note**

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the MLD other querier present interval is 125 x 2 + 10 / 2 = 255 (seconds).

Related commands: **mld timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display mld interface**.

Examples

Set the MLD other querier present interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer other-querier-present 200
```

timer query (MLD view)

Syntax

timer query *interval*

undo timer query

View

MLD view

Default Level

2: System level

Parameters

interval: MLD query interval, namely, amount of time in seconds between MLD general queries, in the range of 1 to 18,000.

Description

Use the **timer query** command to configure the MLD query interval globally.

Use the **undo timer query** command to restore the system default.

By default, the MLD query interval is 125 seconds.

Related commands: **mld timer query**, **timer other-querier-present**, **display mld interface**.

Examples

Set the MLD query interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer query 200
```

version (MLD view)

Syntax

version *version-number*

undo version

View

MLD view

Default Level

2: System level

Parameters

version-number: MLD version number, 1 or 2.

Description

Use the **version** command to configure the MLD version globally.

Use the **undo version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related commands: **mld version**.

Examples

Globally set the MLD version to MLDv2.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] version 2
```

Table of Contents

1 IPv6 PIM Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running IPv6 PIM.

IPv6 PIM Configuration Commands

bsr-policy (IPv6 PIM view)

Syntax

bsr-policy *acl6-number*

undo bsr-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. When an IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source IPv6 address range.

Description

Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely the BSR messages from any source are regarded to be eligible.

Examples

Configure a legal BSR address range so that only routers on the segment 2001::2/64 can become the BSR.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001::2 64
[Sysname-acl6-basic-2000] quit
```

```
[Sysname] pim ipv6
[Sysname-pim6] bsr-policy 2000
```

c-bsr (IPv6 PIM view)

Syntax

c-bsr *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

View

IPv6 PIM view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address of the interface that is to act as a C-BSR.

hash-length: Hash mask length, in the range of 0 to 128. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value means a higher priority.

Description

Use the **c-bsr** command to configure the specified interface a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Note that IPv6 PIM-SM must be enabled on the interface to be configured as a C-BSR.

Related commands: **pim ipv6 sm**, **c-bsr hash-length**, **c-bsr priority**, **c-rp**.

Examples

Configure the interface with an IPv6 address of 1101::1 as a C-BSR.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr 1101::1
```

c-bsr hash-length (IPv6 PIM view)

Syntax

c-bsr hash-length *hash-length*

undo c-bsr hash-length

View

IPv6 PIM view

Default Level

2: System level

Parameters

hash-length: Hash mask length, in the range of 0 to 128.

Description

Use the **c-bsr hash-length** command to configure the global Hash mask length.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length is 126.

Related commands: **c-bsr**.

Examples

Set the global Hash mask length to 16.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr hash-length 16
```

c-bsr holdtime (IPv6 PIM view)

Syntax

c-bsr holdtime *interval*

undo c-bsr holdtime

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: BS timeout in seconds, in the range of 1 to 2,147,483,647.

Description

Use the **c-bsr holdtime** command to configure the BS timeout, namely the length of time for which the C-BSRs wait for a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the BS timeout value is determined by this formula: BS timeout = BS period × 2 + 10.

Note

The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr**, **c-bsr interval**.

Examples

Set the BS timeout to 150 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr holdtime 150
```

c-bsr interval (IPv6 PIM view)

Syntax

c-bsr interval *interval*

undo c-bsr interval

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: BS period in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the c-bsr interval command to configure the BS period, namely the interval at which the BSR sends bootstrap messages.

Use the undo c-bsr interval command to restore the system default.

By default, the BS period value is determined by this formula: BS period = (BS timeout – 10) / 2.

Note

The default BS timeout is 130 seconds, so the default BS period = (130 – 10) / 2 = 60 (seconds).

Related commands: **c-bsr**, **c-bsr holdtime**.

Examples

Set the BS period to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr interval 30
```

c-bsr priority (IPv6 PIM view)

Syntax

c-bsr priority *priority*

undo c-bsr priority

View

IPv6 PIM view

Default Level

2: System level

Parameters

priority: Priority of the C-BSR, in the range of 0 to 255. A larger value means a higher priority.

Description

Use the **c-bsr priority** command to configure the global C-BSR priority.

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

By default, the C-BSR priority is 0.

Related commands: **c-bsr**.

Examples

Set the global C-BSR priority to 5.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr priority 5
```

c-rp (IPv6 PIM view)

Syntax

c-rp *ipv6-address* [**group-policy** *acl6-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *ipv6-address*

View

IPv6 PIM view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address of the interface that is to act as a C-RP.

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. This IPv6 ACL defines a range of IPv6 multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any IPv6 multicast group range that matches the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value means a lower priority.

hold-interval: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not include this argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not include this argument in your command, the corresponding global setting will be used.

Description

Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- IPv6 PIM-SM must be enabled on the interface to be configured as a C-RP.
- If you do not specify an IPv6 multicast group range for the C-RP, the C-RP will serve all IPv6 multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these group ranges in multiple rules in the IPv6 ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

Examples

Configure the interface with the IPv6 address of 2001::1 to be a C-RP for IPv6 multicast group FF0E:0:1391::/96, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff0e:0:1391:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

c-rp advertisement-interval (IPv6 PIM view)

Syntax

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description

Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples

Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp advertisement-interval 30
```

c-rp holdtime (IPv6 PIM view)

Syntax

c-rp holdtime *interval*

undo c-rp holdtime

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description

Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time for which the BSR waits for a C-RP-Adv message from C-RPs.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through bootstrap messages, to prevent loss of C-RP information in bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-rp**, **c-bsr interval**.

Examples

Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp holdtime 200
```

crp-policy (IPv6 PIM view)

Syntax

crp-policy *acl6-number*

undo crp-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Advanced IPv6 ACL number, in the range of 3000 to 3999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies the IPv6 address of a C-RP and the **destination** keyword specifies the IPv6 address range of the IPv6 multicast groups that the C-RP will serve.

Description

Use the **crp-policy** command to configure a legal C-RP address range and the range of served IPv6 multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served IPv6 multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are assumed to be legal.

Note that the **crp-policy** command filters the IPv6 multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the IPv6 multicast group range advertised by a C-RP is FF0E:0:1::/96 while the legal IPv6 multicast group range defined by the **crp-policy** command is FF0E:0:1::/120, the IPv6 multicast groups in the range of FF0E:0:1::/96 are allowed to pass.

Related commands: **c-rp.**

Examples

Configure a C-RP address range so that only routers in the address range of 2001::2/64 can be C-RPs.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 2001::2 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] crp-policy 3000
```

display pim ipv6 bsr-info

Syntax

display pim ipv6 bsr-info

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display pim ipv6 bsr-info** command to view the BSR information in the IPv6 PIM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr**, **c-rp**.

Examples

View the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim ipv6 bsr-info
 Elected BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
     State: Elected
     Uptime: 00:01:10
     Next BSR message scheduled at: 00:00:48
 Candidate BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
     State: Elected

 Candidate RP: 2001::1(LoopBack1)
     Priority: 0
     HoldTime: 130
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
 Candidate RP: 2002::1(Vlan-interface1)
     Priority: 20
     HoldTime: 90
     Advertisement Interval: 50
     Next advertisement scheduled at: 00:00:28
 Candidate RP: 2003::1(Vlan-interface2)
     Priority: 0
     HoldTime: 80
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
```

Table 1-1 display pim ipv6 bsr-info command output description

Field	Description
Elected BSR Address	IPv6 address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Uptime	Length of time since this BSR was elected
Next BSR message scheduled at	Remaining time of this BSR
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval between C-RP-Adv messages
Next BSR message scheduled at	Remaining time before the C-RP will send the next C-RP-Adv message

display pim ipv6 claimed-route

Syntax

display pim ipv6 claimed-route [*ipv6-source-address*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-source-address: Displays the information of the IPv6 unicast route to a particular IPv6 multicast source. If you do not provide this argument, this command will display the information about all IPv6 unicast routes used by IPv6 PIM.

Description

Use the **display pim ipv6 claimed-route** command to view the information of IPv6 unicast routes used by IPv6 PIM.

If an (S, G) is marked SPT, this (S, G) entry uses an IPv6 unicast route.

Examples

View the information of all IPv6 unicast routes used by IPv6 PIM.

```
<Sysname> display pim ipv6 claimed-route
 RPF information about: 2001::2
     RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:100:1
```

```
Referenced prefix/prefix length: 2001::/64
Referenced route type: igp
RPF-route selecting rule: preference-preferred
The (S, G) or (*, G) list dependent on this route entry
(2001::2, FF03::101)
```

Table 1-2 display pim ipv6 claimed-route command output description

Field	Description
RPF information about: 2001::2	Information of the RPF route to IPv6 multicast source 2001::2
RPF interface	RPF interface type and number
RPF neighbor	IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Address/mask of the reference route
Referenced route type	Type of the referenced route: • igp: IGP IPv6 unicast route • egp: EGP IPv6 unicast route • unicast (direct): Direct IPv6 unicast route • unicast: Other IPv6 unicast route (such as IPv6 static unicast route) • mbgp: IPv6 MBGP route
RPF-route selecting rule	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S, G) or (*, G) entry list dependent on this RPF route

display pim ipv6 control-message counters

Syntax

display pim ipv6 control-message counters [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graf**t | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View

Any view

Default Level

1: Monitor level

Parameters

probe: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface-type interface-number: Displays the number of IPv6 PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of graft messages.

graft-ack: Displays the number of graft-ack messages.

hello: Displays the number of hello messages.

join-prune: Displays the number of join/prune messages.

state-refresh: Displays the number of state refresh messages.

Description

Use the **display pim ipv6 control-message counters** command to view the statistics information of IPv6 PIM control messages.

Examples

View the statistics information of all types of IPv6 PIM control messages on all interfaces.

```
<Sysname> display pim ipv6 control-message counters
 PIM global control-message counters:
                  Received         Sent             Invalid
 Register         20               37               2
 Register-Stop    25               20               1
 Probe            10               5                0

 PIM control-message counters for interface: Vlan-interface1
                  Received         Sent             Invalid
 Assert           10               5                0
 Graft            20               37               2
 Graft-Ack        25               20               1
 Hello            1232             453              0
 Join/Prune       15               30               21
 State-Refresh    8                7                1
 BSR              3243             589              1
 C-RP             53               32               0
```

Table 1-3 display pim ipv6 control-message counters command output description

Field	Description
PIM global control-message counters	Statistics of IPv6 PIM global control messages
PIM control-message counters for interface	Interface for which IPv6 PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages

Field	Description
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

display pim ipv6 grafts

Syntax

display pim ipv6 grafts

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display pim ipv6 grafts** command to view the information about unacknowledged graft messages.

Examples

View the information about unacknowledged graft messages.

```
<Sysname> display pim ipv6 grafts
 Source             Group              Age           RetransmitIn
 1004::2            ff03::101          00:00:24      00:00:02
```

Table 1-4 display pim ipv6 grafts command output description

Field	Description
Source	IPv6 multicast source address in the graft message
Group	IPv6 multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

display pim ipv6 interface

Syntax

display pim ipv6 interface [*interface-type interface-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Displays the IPv6 PIM information on a particular interface.

verbose: Displays the detailed PIM information.

Description

Use the **display pim ipv6 interface** command to view the IPv6 PIM information on the specified interface or all interfaces.

Examples

View the detailed IPv6 PIM information on Vlan-interface1.

```
<Sysname> display pim ipv6 interface Vlan-interface 1 verbose
 Interface: Vlan-interface1, FE80::200:5EFF:FE04:8700
     PIM version: 2
     PIM mode: Sparse
     PIM DR: FE80::200:AFF:FE01:101
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on network not using neighbor tracking: 2
```

Table 1-5 display pim ipv6 interface command output description

Field	Description
Interface	Interface name and its IPv6 address
PIM version	IPv6 PIM version
PIM mode	IPv6 PIM mode, dense or sparse
PIM DR	IPv6 address of the DR
PIM DR Priority (configured)	Priority for DR election
PIM neighbor count	Total number of IPv6 PIM neighbors
PIM hello interval	Interval between IPv6 PIM hello messages
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	IPv6 PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim ipv6 join-prune

Syntax

display pim ipv6 join-prune mode { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *ipv6-neighbor-address*] * [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

mode: Displays the information of join/prune messages to send in the specified IPv6 PIM mode. IPv6 PIM modes include **sm** and **ssm**, which represent IPv6 PIM-SM and IPv6 PIM-SSM respectively.

flags *flag-value*: Specifies to display IPv6 PIM routing entries containing the specified flag(s).Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

ipv6-neighbor-address: Displays the information of join/prune messages to send to the specified IPv6 PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

Description

Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Examples

View the information of join/prune messages to send in the IPv6 PIM-SM mode.

```
<Sysname> display pim ipv6 join-prune mode sm

 Expiry Time: 50 sec
 Upstream nbr: FE80::2E0:FCFF:FE03:1004 (Vlan-interface1)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
------------------------------------------------------------------------
 Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 1-6 display pim join-prune command output description

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IPv6 address of the upstream IPv6 PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim ipv6 neighbor

Syntax

display pim ipv6 neighbor [**interface** *interface-type interface-number* | *ipv6-neighbor-address* | **verbose**] *

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Displays the IPv6 PIM neighbor information on a particular interface.

ipv6-neighbor-address: Displays the information of a particular IPv6 PIM neighbor.

verbose: Displays the detailed IPv6 PIM neighbor information.

Description

Use the **display pim ipv6 neighbor** command to view the IPv6 PIM neighbor information.

Examples

View the information of all IPv6 PIM neighbors.

```
<Sysname> display pim ipv6 neighbor
 Total Number of Neighbors = 2

 Neighbor           Interface           Uptime   Expires  Dr-Priority
 FE80::A01:101:1    Vlan1              02:50:49 00:01:31 1
 FE80::A01:102:1    Vlan2              02:49:39 00:01:42 1
```

View the detailed information of the IPv6 PIM neighbor whose IPv6 address is FE80::1.

```
<Sysname> display pim ipv6 neighbor fe80::1 verbose
Neighbor: FE80:: 1
     Interface: Vlan-interface3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
     Generation ID: 0x2ACEFE15
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     State refresh interval: 60 s
     Neighbor tracking: Disabled
```

Table 1-7 display pim ipv6 neighbor command output description

Field	Description
Total Number of Neighbors	Total number of IPv6 PIM neighbors
Neighbor	IPv6 address of the PIM neighbor
Interface	Interface connecting the IPv6 PIM neighbor
Uptime	Length of time since the IPv6 PIM neighbor was discovered
Expires/Expiry time	Remaining time of the IPv6 PIM neighbor; “never” means that the IPv6 PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the IPv6 PIM neighbor
Generation ID	Generation ID of the IPv6 PIM neighbor (a random value indicating status change of the IPv6 PIM neighbor)
Holdtime	Holdtime of the IPv6 PIM neighbor; “forever” means that the IPv6 PIM neighbor is always up and reachable
LAN delay	Prune delay
Override interval	Prune override interval
State refresh interval	Interval of sending state refresh messages
Neighbor tracking	Neighbor tracking status (enabled/disabled)

display pim ipv6 routing-table

Syntax

display pim ipv6 routing-table [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

prefix-length: Prefix length of the IPv6 multicast group/source address prefix. For an IPv6 multicast group address, the effective range is 8 to 128 and the default value is 128; for an IPv6 multicast source address, the effective range is 0 to 128 and the default value is 128.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface.

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

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays routing entries that contain the specified interface as the outgoing interface.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays routing entries of which the outgoing interface list excludes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

mode *mode-type*: Specifies an IPv6 PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies IPv6 PIM-DM.
- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM.

flags *flag-value*: Displays IPv6 PIM routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **act**: Specifies IPv6 multicast routing entries to which actual data has arrived.
- **del**: Specifies IPv6 multicast routing entries scheduled to be deleted.
- **exprune**: Specifies multicast routing entries containing outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext**: Specifies IPv6 routing entries containing outgoing interfaces provided by other IPv6 multicast routing protocols.
- **loc**: Specifies IPv6 multicast routing entries on routers directly connecting to the same subnet with the IPv6 multicast source.
- **niif**: Specifies IPv6 multicast routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies routing entries with IPv6 PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description

Use the **display pim ipv6 routing-table** command to view IPv6 PIM routing table information.

Related commands: **display ipv6 multicast routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

View the content of the IPv6 PIM routing table.

```
<Sysname> display pim ipv6 routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (2001::2, FFE3::101)
     Protocol: pim-dm, Flag:
     UpTime: 00:04:24
     Upstream interface: Vlan-interface1
         Upstream neighbor: FE80::A01:100:1
         RPF prime neighbor: FE80::A01:100:1
```

```
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface2
        Protocol: pim-dm, UpTime: 00:04:24, Expires: 00:02:47
```

Table 1-8 display pim ipv6 routing-table command output description

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the IPv6 PIM routing table
(2001::2, FFE3::101)	An (S, G) entry in the IPv6 PIM routing table
Protocol	IPv6 PIM mode, IPv6 PIM-SM or IPv6 PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the IPv6 PIM routing table
Uptime	Length of time since the (S, G) or (*, G) entry was installed
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry • For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. • For a (S, G) entry, if this router directly connects to the IPv6 multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	Information of the downstream interface(s), including: • Number of downstream interfaces • Downstream interface name • Protocol type configured on the downstream interface • Uptime of the downstream interface(s) • Expiry time of the downstream interface(s)

display pim ipv6 rp-info

Syntax

display pim ipv6 rp-info [*ipv6-group-address*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive. If you do not provide a group address, this command will display the RP information corresponding to all IPv6 multicast groups.

Description

Use the **display pim ipv6 rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Examples

View the RP information corresponding to the IPv6 multicast group FF0E::101.

```
<Sysname> display pim ipv6 rp-info ff0e::101
 PIM-SM BSR RP information:
 prefix/prefix length: FF0E::101/64
     RP: 2004::2
     Priority: 0
     HoldTime: 130
     Uptime: 00:05:19
     Expires: 00:02:11
```

Table 1-9 display pim ipv6 rp-info command output description

Field	Description
prefix/prefix length	The IPv6 multicast group served by the RP
RP	IPv6 address of the RP
Priority	RP priority
HoldTime	Timeout time of the RP
Uptime	Length of time since the RP was elected
Expires	Remaining time of the RP

embedded-rp

Syntax

embedded-rp [*acl6-number*]

undo embedded-rp [*acl6-number*]

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999.

Description

Use the **embedded-rp** command to enable embedded RP.

Use the **undo embedded-rp** command to disable embedded RP or restore the system default.

By default, embedded RP is enabled for IPv6 multicast groups in the default embedded RP address scopes.

Note

The default embedded RP address scopes are FF7x::/12 and FFFx::/12. Here “x” refers to any legal address scope. For details of the scope field, see *Multicast Overview* of the *IP Multicast Volume*.

Note that:

- When you use the **embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be enabled for all the IPv6 multicast groups in the default embedded RP address scopes; if you specify *acl6-number*, the embedded RP feature will be enabled for only those IPv6 multicast groups that are within the default embedded RP address scopes and pass the ACL check.
- When you use the **undo embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be disabled for all the IPv6 multicast groups; if you specify *acl6-number*, this command will restore the system default.

Examples

Enable embedded RP for only those IPv6 multicast groups in the address scope FF7E:140:20::101/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff7e:140:20::101 64
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] embedded-rp 2000
```

hello-option dr-priority (IPv6 PIM view)

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

View

IPv6 PIM view

Default Level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

Description

Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **pim ipv6 hello-option dr-priority**.

Examples

Set the router priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option dr-priority 3
```

hello-option holdtime (IPv6 PIM view)

Syntax

hello-option holdtime *interval*

undo hello-option holdtime

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 means that the IPv6 PIM neighbor is always reachable.

Description

Use the **hello-option holdtime** command to configure the IPv6 PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **pim ipv6 hello-option holdtime**.

Examples

Set the IPv6 PIM neighbor timeout time to 120 seconds globally.

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

```
[Sysname] pim ipv6
[Sysname-pim6] hello-option holdtime 120
```

hello-option lan-delay (IPv6 PIM view)

Syntax

hello-option lan-delay *interval*

undo hello-option lan-delay

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **hello-option override-interval**, **pim ipv6 hello-option override-interval**, **pim ipv6 hello-option lan-delay**.

Examples

Set the LAN-delay to 200 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option lan-delay 200
```

hello-option neighbor-tracking (IPv6 PIM view)

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

View

IPv6 PIM view

Default Level

2: System level

Parameters

None

Description

Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **pim ipv6 hello-option neighbor-tracking**.

Examples

Disable join suppression globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option neighbor-tracking
```

hello-option override-interval (IPv6 PIM view)

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **hello-option lan-delay**, **pim ipv6 hello-option lan-delay**, **pim ipv6 hello-option override-interval**.

Examples

Set the prune override interval to 2,000 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option override-interval 2000
```

holdtime assert (IPv6 PIM view)

Syntax

holdtime assert *interval*

undo holdtime assert

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime join-prune**, **pim ipv6 holdtime assert**.

Examples

Set the global value of the assert timeout time to 100 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime assert 100
```

holdtime join-prune (IPv6 PIM view)

Syntax

holdtime join-prune *interval*

undo holdtime join-prune

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert**, **pim ipv6 holdtime join-prune**.

Examples

Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime join-prune 280
```

jp-pkt-size (IPv6 PIM view)

Syntax

jp-pkt-size *packet-size*

undo jp-pkt-size

View

IPv6 PIM view

Default Level

2: System level

Parameters

packet-size: Maximum size of join/prune messages in bytes, with an effective range of 100 to 64000.

Description

Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

Examples

Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-pkt-size 1500
```

jp-queue-size (IPv6 PIM view)

Syntax

jp-queue-size *queue-size*

undo jp-queue-size

View

IPv6 PIM view

Default Level

2: System level

Parameters

queue-size: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

Description

Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size**, **holdtime join-prune**, **pim holdtime join-prune**.

Examples

Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-queue-size 2000
```

pim ipv6

Syntax

pim ipv6

undo pim ipv6

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6** command to enter IPv6 PIM view.

Use the **undo pim ipv6** command to remove all configurations performed in IPv6 PIM view.

Note that IPv6 multicast routing must be enabled on the device before this command can take effect.

Related commands: **multicast ipv6 routing-enable** (*IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*).

Examples

Enable IPv6 multicast routing and enter IPv6 PIM view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] pim ipv6
[Sysname-pim6]
```

pim ipv6 bsr-boundary

Syntax

pim ipv6 bsr-boundary

undo pim ipv6 bsr-boundary

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 bsr-boundary** command to configure an IPv6 PIM domain border, namely a bootstrap message boundary.

Use the **undo pim ipv6 bsr-boundary** command to remove the configured IPv6 PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr**; **multicast ipv6 boundary** (*IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*).

Examples

Configure VLAN-interface 100 as a PIM domain border.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 bsr-boundary
```

pim ipv6 dm

Syntax

pim ipv6 dm

undo pim ipv6 dm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 dm** command to enable IPv6 PIM-DM.

Use the **undo pim ipv6 dm** command to disable IPv6 PIM-DM.

By default, IPv6 PIM-DM is disabled.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

Related commands: **pim ipv6 sm**, **ssm-policy**; **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IPv6 multicast routing, and enable IPv6 PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 dm
```

pim ipv6 hello-option dr-priority

Syntax

pim ipv6 hello-option dr-priority *priority*

undo pim ipv6 hello-option dr-priority

View

Interface view

Default Level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

Description

Use the **pim ipv6 hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim ipv6 hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

Examples

Set the router priority for DR election to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option dr-priority 3
```

pim ipv6 hello-option holdtime

Syntax

pim ipv6 hello-option holdtime *interval*

undo pim ipv6 hello-option holdtime

View

Interface view

Default Level

2: System level

Parameters

interval: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 means that the PIM neighbor is always reachable.

Description

Use the **pim ipv6 hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim ipv6 hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

Examples

Set the IPv6 PIM neighbor timeout time to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option holdtime 120
```

pim ipv6 hello-option lan-delay

Syntax

pim ipv6 hello-option lan-delay *interval*

undo pim ipv6 hello-option lan-delay

View

Interface view

Default Level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use the **pim ipv6 hello-option lan-delay** command to configure the LAN-delay time, namely the device waits between receiving a prune message and taking a prune action, on the current interface.

Use the **undo pim ipv6 hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **pim ipv6 hello-option override-interval**, **hello-option override-interval**, **hello-option lan-delay**.

Examples

Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option lan-delay 200
```

pim ipv6 hello-option neighbor-tracking

Syntax

pim ipv6 hello-option neighbor-tracking

undo pim ipv6 hello-option neighbor-tracking

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim ipv6 hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

Examples

Disable join suppression on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option neighbor-tracking
```

pim ipv6 hello-option override-interval

Syntax

pim ipv6 hello-option override-interval *interval*

undo pim ipv6 hello-option override-interval

View

Interface view

Default Level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use the **pim ipv6 hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim ipv6 hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **pim ipv6 hello-option lan-delay**, **hello-option lan-delay**, **hello-option override-interval**.

Examples

Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option override-interval 2000
```

pim ipv6 holdtime assert

Syntax

pim ipv6 holdtime assert *interval*

undo pim ipv6 holdtime assert

View

Interface view

Default Level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use the **pim ipv6 holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim ipv6 holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime join-prune**, **holdtime assert**.

Examples

Set the assert timeout time to 100 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime assert 100
```

pim ipv6 holdtime join-prune

Syntax

pim ipv6 holdtime join-prune *interval*

undo pim ipv6 holdtime join-prune

View

Interface view

Default Level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use the **pim ipv6 holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim ipv6 holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert**, **holdtime join-prune**.

Examples

Set the join/prune timeout time to 280 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] pim ipv6 holdtime join-prune 280
```

pim ipv6 require-genid

Syntax

pim ipv6 require-genid

undo pim ipv6 require-genid

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 require-genid** command enable rejection of hello messages without Generation_ID.

Use the **undo pim ipv6 require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Examples

Enable VLAN-interface 100 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 require-genid
```

pim ipv6 sm

Syntax

pim ipv6 sm

undo pim ipv6 sm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 sm** command to enable IPv6 PIM-SM.

Use the **undo pim ipv6 sm** command to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

Note that this command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **pim ipv6 dm**; **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples

Enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 sm
```

pim ipv6 state-refresh-capable

Syntax

pim ipv6 state-refresh-capable

undo pim ipv6 state-refresh-capable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim ipv6 state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, **state-refresh-hoplimit**.

Examples

Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim ipv6 state-refresh-capable
```

pim ipv6 timer graft-retry

Syntax

pim ipv6 timer graft-retry *interval*

undo pim ipv6 timer graft-retry

View

Interface view

Default Level

2: System level

Parameters

interval: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description

Use the **pim ipv6 timer graft-retry** command to configure the graft retry period.

Use the **undo pim ipv6 timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

Examples

Set the graft retry period to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer graft-retry 80
```

pim ipv6 timer hello

Syntax

pim ipv6 timer hello *interval*

undo pim ipv6 timer hello

View

Interface view

Default Level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **pim ipv6 timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim ipv6 timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

Examples

Set the hello interval to 40 seconds on VLAN-interface 100.

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

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer hello 40
```

pim ipv6 timer join-prune

Syntax

pim ipv6 timer join-prune *interval*

undo pim ipv6 timer join-prune

View

Interface view

Default Level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **pim ipv6 timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim ipv6 timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

Examples

Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer join-prune 80
```

pim ipv6 triggered-hello-delay

Syntax

pim ipv6 triggered-hello-delay *interval*

undo pim ipv6 trigged-hello-delay

View

Interface view

Default Level

2: System level

Parameters

interval: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

Description

Use the **pim ipv6 triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim ipv6 triggered-hello-delay** command to restore the system default.

By default, the maximum delay between hello messages is 5 seconds.

Examples

Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 trigged-hello-delay 3
```

probe-interval (IPv6 PIM view)

Syntax

probe-interval *interval*

undo probe-interval

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Register probe time in seconds, with an effective range of 1 to 1799.

Description

Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the system default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples

Set the register probe time to 6 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] probe-interval 6
```

register-policy (IPv6 PIM view)

Syntax

register-policy *acl6-number*

undo register-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Advanced IPv6 ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the IPv6 ACL can be accepted by the RP.

Description

Use the **register-policy** command to configure an IPv6 ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

Examples

Configure a register filtering policy on the RP so that the RP will accept only those register messages from IPv6 multicast sources on the 3:1::/64 subnet for IPv6 multicast groups on the FF0E:13::/64 subnet.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 3:1:: 64 destination ff0e:13:: 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] register-policy 3000
```

register-suppression-timeout (IPv6 PIM view)

Syntax

register-suppression-timeout *interval*

undo register-suppression-timeout

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Register suppression time in seconds, in the range of 1 to 3,600.

Description

Use the **register-suppression-timeout** command to configure the register suppression time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval**, **register-policy**.

Examples

Set the register suppression time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-suppression-timeout 70
```

register-whole-checksum (IPv6 PIM view)

Syntax

register-whole-checksum

undo register-whole-checksum

View

IPv6 PIM view

Default Level

2: System level

Parameters

None

Description

Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based only on the header in the register message.

Related commands: **register-policy**, **register-suppression-timeout**.

Examples

Configure the router to calculate the checksum based on the entire register message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-whole-checksum
```

reset pim ipv6 control-message counters

Syntax

reset pim ipv6 control-message counters [**interface** *interface-type interface-number*]

View

User view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies to reset the IPv6 PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information about IPv6 PIM control messages on all interfaces.

Description

Use the **reset pim ipv6 control-message counters** command to reset IPv6 PIM control message counters.

Examples

Reset IPv6 PIM control message counters on all interfaces.

```
<Sysname> reset pim ipv6 control-message counters
```

source-lifetime (IPv6 PIM view)

Syntax

source-lifetime *interval*

undo source-lifetime

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: IPv6 multicast source lifetime in seconds, with an effective range of 1 to 65,535.

Description

Use the **source-lifetime** command to configure the IPv6 multicast source lifetime.

Use the **undo source-lifetime** command to restore the system default.

By default, the lifetime of an IPv6 multicast source is 210 seconds.

Examples

Set the IPv6 multicast source lifetime to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] source-lifetime 200
```

source-policy (IPv6 PIM view)

Syntax

source-policy *acl6-number*

undo source-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999.

Description

Use the **source-policy** command to configure an IPv6 multicast data filter.

Use the **undo source-policy** command to remove the configured IPv6 multicast data filter.

By default, no IPv6 multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received IPv6 multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received IPv6 multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Examples

Configure the router to accept IPv6 multicast packets originated from 3121::1 and discard IPv6 multicast packets originated from 3121::2.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 3121::1 128
[Sysname-acl6-basic-2000] rule deny source 3121::2 128
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] source-policy 2000
[Sysname-pim6] quit
```

spt-switch-threshold infinity (IPv6 PIM view)

Syntax

spt-switch-threshold infinity [**group-policy** *acl6-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl6-number*]

View

IPv6 PIM view

Default Level

2: System level

Parameters

group-policy *acl6-number*: Specifies a basic IPv6 ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the configuration will apply on all IPv6 multicast groups.

order *order-value*: Specifies the order of the IPv6 ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the IPv6 ACL in the group-policy list. If you have assigned an *order-value* to a certain IPv6 ACL, do not specify the same *order-value* for another IPv6 ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the IPv6 ACL will remain the same in the group-policy list.

Description

Use the **spt-switch-threshold infinity** command to configure disabling the SPT switchover.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet.

Note that:

- To adjust the order of an IPv6 ACL that already exists in the group-policy list, you can use the acl6-number argument to specify this IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. The order of the other existing IPv6 ACLs in the group-policy list will remain unchanged.
- To use an IPv6 ACL that does not exist in the group-policy list, you can use the acl6-number argument to specify an IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. If you do not include the order order-value option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same IPv6 multicast group, the first traffic rate configuration matched in sequence will take effect.
- For an S7900E series Ethernet switch, once an IPv6 multicast forwarding entry is created, subsequent IPv6 multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not use the **spt-switch-threshold infinity** command on a switch that may become an RP (namely, a static RP or a C-RP).

Examples

Disable SPT switchover on a switch that will never become an RP.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold infinity
```

ssm-policy (IPv6 PIM view)

Syntax

ssm-policy *acl6-number*

undo ssm-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999.

Description

Use the **ssm-policy** command to configure the IPv6 SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the IPv6 SSM group range is FF3x::/32. Here x refers to any legal scope.

This command allows you to define an address range of permitted or denied IPv6 multicast groups. If the match succeeds, the running multicast mode will be IPv6 PIM-SSM; otherwise the multicast mode will be IPv6 PIM-SM.

Examples

Configure the IPv6 SSM group range to be FF3E:0:8192::/96.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff3e:0:8192:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] ssm-policy 2000
```

state-refresh-hoplimit

Syntax

state-refresh-hoplimit *hoplimit-value*

undo state-refresh-hoplimit

View

IPv6 PIM view

Default Level

2: System level

Parameters

hoplimit-value: Hop limit value of state refresh messages, in the range of 1 to 255.

Description

Use the **state-refresh-hoplimit** command to configure the hop limit value of state refresh messages.

Use the **undo state-refresh-hoplimit** command to restore the system default.

By default, the hop limit value of state refresh messages is 255.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, **state-refresh-rate-limit**.

Examples

Set the hop limit value of state refresh messages to 45.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-hoplimit 45
```

state-refresh-interval (IPv6 PIM view)

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: State refresh interval in seconds, with an effective range of 1 to 255.

Description

Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-rate-limit**, **state-refresh-hoplimit**.

Examples

Set the state refresh interval to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-interval 70
```

state-refresh-rate-limit (IPv6 PIM view)

Syntax

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description

Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, **state-refresh-hoplimit**.

Examples

Configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-rate-limit 45
```

static-rp (IPv6 PIM view)

Syntax

static-rp *ipv6-rp-address* [*acl6-number*] [**preferred**]

undo static-rp *ipv6-rp-address*

View

IPv6 PIM view

Default Level

2: System level

Parameters

ipv6-rp-address: IPv6 address of the static RP to be configured. This address must be a valid, globally scoped IPv6 unicast address.

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those IPv6 multicast groups that pass the filtering; otherwise, the configured static RP will serve the all IPv6 multicast groups.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

Description

Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- IPv6 PIM-SM or IPv6 PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the IPv6 ACL rule applied on a static RP changes, a new RP must be elected for all IPv6 multicast groups.
- You can configure multiple static RPs by carrying out this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same IPv6 ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same IPv6 multicast group, the one with the highest IPv6 address will be chosen to serve the group.
- You can configure up to 50 static RPs on the same device.

Related commands: **display pim ipv6 rp-info**.

Examples

Configure the interface with an IPv6 address of 2001::2 as a static RP.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] static-rp 2001::2
```

timer hello (IPv6 PIM view)

Syntax

timer hello *interval*

undo timer hello

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **timer hello** command to configure the hello interval globally.

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

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim ipv6 timer hello**.

Examples

Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer hello 40
```

timer join-prune (IPv6 PIM view)

Syntax

timer join-prune *interval*

undo timer join-prune

View

IPv6 PIM view

Default Level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim ipv6 timer join-prune**.

Examples

Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer join-prune 80
```

Table of Contents

1 IPv6 MBGP Configuration Commands

IPv6 MBGP Configuration Commands

balance (IPv6 MBGP address family view)

Syntax

balance *number*

undo balance

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

maximum: Number of IPv6 MBGP routes for load balancing, in the range 1 to 4. When it is set to 1, load balancing is disabled.

Description

Use the **balance** command to configure the number of IPv6 MBGP routes used for load balancing.

Use the **undo balance** command to disable load balancing.

By default, load balancing is disabled.

Unlike IGP, IPv6 MBGP has no explicit metric for making load balancing decisions. Instead, it implements load balancing by using IPv6 MBGP route selection rules.

Related commands: **display ipv6 multicast routing-table**.

Examples

In IPv6 MBGP address family view, set the number of IPv6 MBGP routes for load balancing to 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] balance 2
```

bestroute as-path-neglect (IPv6 MBGP address family view)

Syntax

bestroute as-path-neglect

undo bestroute as-path-neglect

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute as-path-neglect** command to configure IPv6 MBGP not to consider the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure IPv6 MBGP to consider the AS_PATH during best route selection.

By default, IPv6 MBGP considers the AS_PATH during best route selection.

Examples

In IPv6 MBGP address family view, configure IPv6 MBGP to ignore the AS_PATH during best route selection.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]bestroute as-path-neglect
```

bestroute compare-med (IPv6 MBGP address family view)

Syntax

bestroute compare-med

undo bestroute compare-med

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

By default, the comparison of the MED for paths from each AS is disabled.

Caution

After the **bestroute compare-med** command is used, the **balance** command will not take effect.

Examples

In IPv6 MBGP address family view, enable the comparison of MED for paths from each AS during best route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] bestroute compare-med
```

bestroute med-confederation (IPv6 MBGP address family view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

Such comparison is disabled by default.

With this command used, the system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]bestroute med-confederation
```

compare-different-as-med (IPv6 MBGP address family view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

By default, MED comparison is not allowed among the routes from the peers in different ASs.

If there are several paths for one destination available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP and routing selection method.

Examples

In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]compare-different-as-med
```

dampening (IPv6 MBGP address family view)

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

half-life-reachable: Specifies the half-life for reachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies the half-life for unreachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies the reuse threshold value for suppressed routes, in the range 1 to 20000. A suppressed route having the penalty value decreased under the value is reused. By default, the value is 750.

suppress: Threshold for a route to be suppressed, in the range 1 to 20000. A route is suppressed if its penalty value exceeds this value. The value must be greater than the *reuse* value. By default, the value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be greater than the *suppress* value. The default is 16000.

route-policy-name: Route policy name, a string of 1 to 19 characters.

half-life-reachable, half-life-unreachable, reuse, suppress, and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description

Use the **dampening** command to configure IPv6 MBGP route dampening.

Use the **undo dampening** command to disable route dampening.

By default, route dampening is not configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 multicast routing-table dampened**, **display bgp ipv6 multicast routing-table dampening parameter**, **display bgp ipv6 multicast routing-table flap-info**.

Examples

In IPv6 MBGP address family view, configure route dampening.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]dampening 15 15 1000 2000 10000
```

default local-preference (IPv6 MBGP address family view)

Syntax

default local-preference *value*

undo default local-preference

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

value: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default local preference is 100.

Using this command can affect IPv6 MBGP route selection.

Examples

In IPv6 MBGP address family view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default local-preference 180
```

default med (IPv6 MBGP address family view)

Syntax

default med *med-value*

undo default med

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

med-value: Default MED value, in the range 0 to 4294967295.

Description

Use the **default med** command to specify the default MED value.

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

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from the local preference, the MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all the other conditions are the same, the system selects the route with the lowest MED as the best external route.

Examples

Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default med 25
```

default-route imported (IPv6 MBGP address family view)

Syntax

default-route imported

undo default-route imported

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **default-route imported** command to enable default route redistribution into the IPv6 MBGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, default route redistribution is disabled.

Examples

Enable default and OSPFv3 route redistribution into IPv6 MBGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default-route imported
[Sysname-bgp-af-ipv6-mul] import-route ospfv3 1
```

display ipv6 multicast routing-table

Syntax

display ipv6 multicast routing-table [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays brief information about active IPv6 MBGP routes only.

Description

Use the **display ipv6 multicast routing-table** command to display the IPv6 MBGP routing table.

There are active and inactive routes in the IPv6 MBGP routing table. Active routes are the optimal routes used for RPF check.

Examples

Display brief IPv6 MBGP routing table information.

```
<Sysname> display ipv6 multicast routing-table
Routing Table :
        Destinations : 1        Routes : 1

Destination :  ::1                                  PrefixLength : 128
NextHop      : ::1                                  Preference : 0
Interface    : InLoopBack0                          Protocol    : Direct
State        : Active NoAdv                         Cost        : 0
Tunnel ID    : 0x0                                  Label       : NULL
Age          : 156sec
```

Table 1-1 display ipv6 multicast routing-table command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop IP address
Preference	Route preference
Interface	Outbound interface
Protocol	Routing protocol
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv
Cost	Route cost
Tunnel ID	Tunnel ID
Label	Label
Age	Time elapsed since the route was generated

Display detailed IPv6 MBGP routing table information.

```
<Sysname> display ipv6 multicast 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           : 17073sec
```

Table 1-2 display ipv6 multicast routing-table verbose command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop IP address
Preference	Route preference
RelayNextHop	Recursive next hop
Tag	Route tag
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv
Cost	Route cost
Tunnel ID	Tunnel ID
Label	Label
Age	Time elapsed since the route was generated

display ipv6 multicast routing-table *ipv6-address prefix-length*

Syntax

display ipv6 multicast 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 routes matching the specified prefix.

verbose: Displays both detailed active and inactive routing information permitted by the ACL. Without this keyword, only the brief information about active routes permitted by the ACL is displayed.

Description

Use the **display ipv6 multicast routing-table** *ipv6-address prefix-length* command to display the multicast routing information for the specified destination IPv6 address.

Examples

Display brief information about the specified multicast route.

```
<Sysname> display ipv6 multicast routing-table 4::1 32
Routing Table:
Summary Count 1
  Destination : 4::                          PrefixLength : 32
  NextHop     : 3::1                         Preference   : 60
  Interface   : Vlan-interface1                 Protocol     : Static
  State       : Active Adv                   Cost         : 0
  Tunnel ID   : 0x0                          Label        : NULL
  Age         : 19174sec
```

Display the brief route information falling into the specified network.

```
<Sysname> display ipv6 multicast  routing-table 4:: 16 longer-match
Routing Tables:
Summary Count 2
Destination  : 4::                          PrefixLength  : 32
NextHop      : 3::1                         Preference    : 60
Interface    : Vlan-interface1                 Protocol      : Static
State        : Active Adv                   Cost          : 0
Tunnel ID    : 0x0                          Label         : NULL
Age          : 766sec

Destination   : 4:4::                       PrefixLength : 64
NextHop       : 3::1                         Preference   : 60
Interface     : Vlan-interface1                 Protocol     : Static
State         : Active Adv                   Cost         : 0
Tunnel ID     : 0x0                          Label        : NULL
Age           : 766sec
```

Display the detailed route information falling into the specified network.

```
<Sysname> display ipv6 multicast  routing-table 4:4:: 32 verbose
Routing Tables:
Summary count:1
Destination  : 4:4::                          PrefixLength : 64
NextHop      : 3::1                         Preference    : 60
Interface    : Vlan-interface1                 Protocol      : Static
State        : Active Adv                   Cost          : 0
Age          : 19547sec
```

display bgp ipv6 multicast group

Syntax

display bgp ipv6 multicast group [*ipv6-group-name*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-name: Peer group name, a string of 1 to 47 characters.

Description

Use the **display bgp ipv6 multicast group** command to display IPv6 MBGP peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples

Display information about the IPv6 MBGP peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa

 BGP peer-group is aaa
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer         V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  20:20::20:1  4   200       170       141      0        2 02:13:35 Established
```

Table 1-3 display bgp ipv6 multicast group command output description

Field	Description
BGP peer-group	Name of the IPv6 MBGP peer group
remote AS	AS number of the IPv6 MBGP peer group
Type	Type of the IPv6 MBGP peer group:
Maximum allowed prefix number	Maximum number of prefixes allowed to receive from the IPv6 MBGP peer group
Threshold	Threshold value

Field	Description
Configured hold timer value	Hold timer value
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisement
Peer Preferred Value	Preferred value of the routes from the peer
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state machine

display bgp ipv6 multicast network

Syntax

display bgp ipv6 multicast network

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 multicast network** command to display the IPv6 MBGP routes advertised with the **network** command.

Examples

Display IPv6 MBGP routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 multicast network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask            Route-policy        Short-cut
```

```
2002::           64
2001::           64                                    Short-cut
```

Table 1-4 display bgp ipv6 multicast network command output description

Field	Description
BGP Local Router ID	BGP local router ID
Local AS Number	Local AS number
Network	Network address
Mask	Prefix length of the address
Route-policy	Route policy configured
Short-cut	Shortcut route

display bgp ipv6 multicast paths

Syntax

display bgp ipv6 multicast paths [*as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression.

Description

Use the **display bgp ipv6 multicast paths** command to display AS path information.

If no parameter is specified, all AS path information will be displayed.

Examples

Display AS path information.

```
<Sysname> display bgp ipv6 multicast paths

    Address       Hash    Refcount  MED         Path/Origin
    0x5917098     1       1          0            i
    0x59171D0     9       2          0            100i
```

Table 1-5 display bgp ipv6 multicast paths command output description

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation
Hash	Hash index

Field	Description	
Refcount	Count of routes that referenced the path	
MED	MED of the path	
Path	AS_PATH attribute of the route, recording the ASs it has passed, used to avoid routing loops	
Origin	Origin attribute of the route:	
	I	Indicates the route is interior to the AS. Summary routes and routes injected with the **network** command are considered IGP routes.
	E	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	It indicates that the origin of the route is unknown and the route is learned by some other means. BGP sets the Origin attribute of routes learned from other IGP protocols to incomplete.

display bgp ipv6 multicast peer

Syntax

display bgp ipv6 multicast peer [[*ipv6-address*] **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer to be displayed.

ipv6-address: IPv6 address of a peer to be displayed.

log-info: Displays the log information of the specified peer.

verbose: Displays the detailed information of the peer.

Description

Use the **display bgp ipv6 multicast peer** command to display IPv6 MBGP peer/peer group information.

If no parameter is specified, information about all IPv6 MBGP peers and peer groups is displayed.

Examples

Display all IPv6 MBGP peer information.

```
<Sysname> display bgp ipv6 multicast peer
```

```
 BGP Local router ID : 20.0.0.1
 local AS number : 100
Total number of peers : 1                 Peers in established state : 1

Peer      V    AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down    State

20::21    4   200  17       19       0          3  00:09:59   Established
```

Table 1-6 display bgp ipv6 multicast peer command output description

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of the session/the lasting time of the present state (when no session is established)
State	Peer state machine

display bgp ipv6 multicast routing-table

Syntax

display bgp ipv6 multicast routing-table [*ipv6-address prefix-length*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

Description

Use the **display bgp ipv6 multicast routing-table** command to display IPv6 MBGP routing information.

Examples

Display IPv6 MBGP routing information.

```
<Sysname> display bgp ipv6 routing-table
```

```
Total Number of Routes: 2

BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*>  Network : 30:30::                                  PrefixLen : 64
    NextHop : 30:30::30:1                              LocPrf    :
    PrefVal : 0                                        Label     : NULL
    MED     : 0
    Path/Ogn: i

*>  Network : 40:40::                                  PrefixLen : 64
    NextHop : 40:40::40:1                              LocPrf    :
    PrefVal : 0                                        Label     : NULL
    MED     : 0
    Path/Ogn: i
```

Table 1-7 display bgp ipv6 multicast routing-table command output description

Field	Description
Local router ID	Local router ID
Status codes	Status codes: * - valid: valid route > - best: best route d – damped: dampened route h – history: history route i – internal: internal route s – suppressed: suppressed route S – Stale: stale route
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by some other means)
Network	Destination network address
PrefixLen	Prefix length of the address
NextHop	Next hop IP address
MED	MULTI_EXIT_DISC attribute value
LocPrf	Local precedence
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops
PrefVal	Preferred value for a route
Label	Label

Field	Description	
Ogn	Origin attribute of the route:	
	i	Indicates the route is interior to the AS. Summary routes and routes injected with the **network** command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	It indicates that the origin of the route is unknown and the route is learned by some other means. BGP sets the Origin attribute of routes learned from other IGP protocols to incomplete.

display bgp ipv6 multicast routing-table as-path-acl

Syntax

display bgp ipv6 multicast routing-table as-path-acl *as-path-acl-number*

View

Any view

Default Level

1: Monitor level

Parameters

as-path-acl-number: Displays routing information matching an AS path ACL numbered 1 to 256

Description

Use the **display bgp ipv6 multicast routing-table as-path-acl** command to display the IPv6 MBGP routes matching the specified AS path ACL.

Examples

Display the IPv6 MBGP routes matching AS path ACL 20.

```
<Sysname> display bgp ipv6 multicast routing-table as-path-acl 20
 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 1-7 for description on the fields above.

display bgp ipv6 multicast routing-table community

Syntax

display bgp ipv6 multicast routing-table community [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View

Any view

Default Level

1: Monitor level

Parameters

aa:nn: Community number; both *aa* and *nn* are in the range 0 to 65535.

&<1-13>: Indicates that you can provide up to 13 community numbers.

no-advertise: Displays IPv6 MBGP routes that cannot be advertised to any peer.

no-export: Displays IPv6 MBGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub-ASs in the confederation.

no-export-subconfed: Displays IPv6 MBGP routes that cannot be advertised out the local AS, or to other sub-ASs in the confederation.

whole-match: Displays the IPv6 MBGP routes exactly matching the specified community attribute.

Description

Use the **display bgp ipv6 multicast routing-table community** command to display the IPv6 MBGP routing information with the specified IPv6 MBGP community attribute.

Examples

Display IPv6 MBGP routing information with the community attribute **no-export**.

```
<Sysname> display bgp ipv6 multicast routing-table community no-export
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 1-7 for description on the fields above.

display bgp ipv6 multicast routing-table community-list

Syntax

display bgp ipv6 multicast routing-table community-list { *basic-community-number* [**whole-match**] | *adv-community-number* }&<1-16>

View

Any view

Default Level

1: Monitor level

Parameters

basic-community-number: Basic community-list number, in the range 1 to 99.

adv-community-number: Advanced community-list number, in the range 100 to 199.

whole-match: Displays the IPv6 MBGP routes exactly matching the community attributes defined in the specified *basic-community-number*.

&<1-16>: Indicates that you can enter the preceding argument up to 16 times.

Description

Use the **display bgp ipv6 multicast routing-table community-list** command to display the IPv6 MBGP routing information matching the specified IPv6 MBGP community list.

Examples

Display the IPv6 MBGP routing information matching the community list

```
<Sysname> display bgp ipv6 multicast routing-table community-list 99
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                PrefixLen : 64
     NextHop : 30:30::30:1                            LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 1-7 for description on the fields above.

display bgp ipv6 multicast routing-table dampened

Syntax

display bgp ipv6 multicast routing-table dampened

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 multicast routing-table dampened** command to display the dampened IPv6 MBGP routes.

Examples

Display dampened IPv6 MBGP routing information

```
<Sysname> display bgp ipv6 multicast routing-table dampened

BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network : 111::                                PrefixLen : 64
     From    : 122::1                               Reuse     : 00:29:34
     Path/Ogn: 200?
```

Table 1-8 display bgp ipv6 multicast routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Route reuse time, namely, period of time before the unusable route becomes usable.

Refer to Table 1-7 for description on the other fields above.

display bgp ipv6 multicast routing-table dampening parameter

Syntax

display bgp ipv6 multicast routing-table dampening parameter

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 multicast routing-table dampening parameter** command to display IPv6 MBGP routing dampening parameters.

Related commands: **dampening**.

Examples

Display IPv6 MBGP dampening parameter information.

```
<Sysname> display bgp ipv6 multicast routing-table dampening parameter
 Maximum Suppress Time(in second)     : 3069
 Ceiling Value                        : 16000
 Reuse Value                          : 750
 Reach HalfLife Time(in second)  : 900
 Unreach HalfLife Time(in second): 900
 Suppress-Limit                       : 2000
```

Table 1-9 display bgp ipv6 multicast routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum suppress time
Ceiling Value	Ceiling penalty value
Reuse Value	Limit for a route to be desuppressed
Reach HalfLife Time(in second)	Half-life of reachable routes
Unreach HalfLife Time(in second)	Half-life of unreachable routes
Suppress-Limit	Limit for routes to be suppressed

display bgp ipv6 multicast routing-table different-origin-as

Syntax

display bgp ipv6 multicast routing-table different-origin-as

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 multicast routing-table different-origin-as** command to display IPv6 MBGP routes originating from different autonomous systems.

Examples

Display IPv6 MBGP routing information from different ASs

```
<Sysname> display bgp ipv6 multicast routing-table different-origin-as

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 222::                                  PrefixLen : 64
     NextHop : 122::2                                 LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: 100 ?
```

For details about the displayed information, see Table 1-7.

display bgp ipv6 multicast routing-table flap-info

Syntax

display bgp ipv6 multicast routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ipv6-address* [*prefix-length* [**longer-match**]]]

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression to be matched.

as-path-acl-number: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

ipv6-address: IPv6 address of a route to be displayed.

prefix-length: Prefix length of the IPv6 address, in the range 1 to 128.

longer-match: Matches the longest prefix.

Description

Use the **display bgp ipv6 multicast routing-table flap-info** command to display IPv6 MBGP route flap statistics.

Examples

Display IPv6 MBGP routing flap statistics

```
<Sysname> display bgp ipv6 multicast routing-table flap-info

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
```

```
                h - history,  i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network  : 111::                                PrefixLen : 64
     From     : 122::1                               Flaps     : 3
     Duration : 00:13:47                             Reuse     : 00:16:36
     Path/Ogn : 200?
```

Table 1-10 display bgp ipv6 multicast routing-table flap-info command output description

Field	Description
Flaps	Number of flaps
Duration	Duration of the flapping
Reuse	Reuse value

Refer to Table 1-7 for description on the other fields above.

display bgp ipv6 multicast routing-table peer

Syntax

display bgp ipv6 multicast routing-table peer *ipv6-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

statistic: Displays route statistics.

Description

Use the **display bgp ipv6 multicast routing-table peer** command to display the routing information advertised to or received from the specified IPv6 MBGP peer.

Examples

Display the routing information advertised to the specified IPv6 MBGP peer.

```
<Sysname> display bgp ipv6 multicast routing-table peer 10:10::10:1 advertised-routes
 Total Number of Routes: 2

 BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*>  Network : 20:20::                                  PrefixLen : 64
    NextHop : 20:20::20:1                              LocPrf    :
    PrefVal : 0                                        Label     : NULL
    MED     : 0
    Path/Ogn: i

*>  Network : 40:40::                                  PrefixLen : 64
    NextHop : 30:30::30:1                              LocPrf    :
    PrefVal : 0                                        Label     : NULL
    MED     : 0
    Path/Ogn: 300 i
```

Refer to Table 1-7 for description on the fields above.

display bgp ipv6 multicast routing-table regular-expression

Syntax

display bgp ipv6 multicast routing-table regular-expression *as-regular-expression*

View

Any view

Default Level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression.

Description

Use the **display bgp ipv6 multicast routing-table regular-expression** command to display the IPv6 MBGP routes matching the specified AS regular expression.

Examples

Display IPv6 MBGP routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 multicast routing-table regular-expression ^100

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*>  Network : 50:50::                                  PrefixLen : 64
    NextHop : 10:10::10:1                              LocPrf    :
    PrefVal : 0                                        Label     : NULL
```

```
MED     : 0
Path/Ogn: 100 i
```

Refer to Table 1-7 for description on the fields above.

display bgp ipv6 multicast routing-table statistic

Syntax

display bgp ipv6 multicast routing-table statistic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display bgp ipv6 multicast routing-table statistic** command to display IPv6 MBGP routing statistics.

Examples

Display IPv6 MBGP routing statistics

```
<Sysname> display bgp ipv6 multicast routing-table statistic

 Total Number of Routes: 1
```

filter-policy export (IPv6 MBGP address family view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of a basic or advanced ACL used to match against the destination of routing information. The number is in the range 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

Description

Use the **filter-policy export** command to filter outgoing routes using a specified filter.

Use the **undo filter-policy export** command to cancel the filtering of outgoing routes.

By default, no outgoing routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes are filtered.

Examples

Reference IPv6 ACL 2001 to filter all outgoing IPv6 MBGP routes.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]filter-policy 2001 export
```

filter-policy import (IPv6 MBGP address family view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of a basic or advanced IPv6 ACL used to match against the destination of routing information. The number is in the range 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to configure the filtering of inbound routing information using a specified filter.

Use the **undo filter-policy import** command to cancel the filtering of inbound routing information.

By default, inbound IPv6 MBGP routes are not filtered.

Examples

Reference IPv6 ACL 2000 to filter all inbound IPv6 MBGP routes.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] filter-policy 2000 import
```

import-route (IPv6 MBGP address family view)

Syntax

import-route *protocol* [*process-id*] [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

protocol: Redistributes routes from the protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present.

process-id: Process ID. It ranges from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

med-value: Default MED value, in the range 0 to 4294967295. If no MED is specified, the cost of a redistributed route will be used as its MED in the BGP routing domain.

route-policy-name: Name of a route policy used to filter redistributed routes, a string of 1 to 19 characters.

Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, IPv6 MBGP does not redistribute routes from any routing protocol.

The origin attribute of routes redistributed with the **import-route** command is incomplete.

Examples

Redistribute routes from RIPng 1.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] import-route ripng 1
```

ipv6-family multicast

Syntax

ipv6-family multicast

undo ipv6-family multicast

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6-family** command to enter IPv6 MBGP address family view.

Use the **undo ipv6-family** command to remove all the configurations in the IPv6 MBGP address family view.

IPv4 BGP unicast view is the default.

Examples

Enter IPv6 MBGP address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]
```

network (IPv6 MBGP address family view)

Syntax

network *ipv6-address prefix-length* [**route-policy** *route-policy-name* | **short-cut**]

undo network *ipv6-address prefix-length* [**short-cut**]

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

short-cut: If the keyword is specified for an IPv6 multicast eBGP route, the route will use the local preference rather than its own preference, and therefore it will hardly become the optimal route.

route-policy-name: Name of a route policy, a string of 1 to 19 characters.

Description

Use the **network** command to inject a network to the IPv6 MBGP routing table.

Use the **undo network** command to remove a network from the routing table.

By default, no network is injected.

Note the following:

- The network to be injected must exist in the local IPv6 routing table. You can use a route policy to control the advertisement of the route with more flexibility.
- The route injected with the **network** command has the IGP origin attribute.

Examples

inject the network 2002::/16.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] network 2002:: 16
```

peer advertise-community (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **advertise-community**

undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-community**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer advertise-community** command to advertise the community attribute to an IPv6 MBGP peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any IPv6 MBGP peer group/peer.

Examples

Advertise the community attribute to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**

undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to an IPv6 MBGP peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to any IPv6 MBGP peer/peer group.

Examples

Advertise the extended community attribute to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **allow-as-loop** [*number*]

undo peer { *ipv6-group-name* | *ipv6-address* } **allow-as-loop**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

number: Specifies the number of times for which the local AS number can appear in the AS PATH of routes from the peer/peer group, in the range 1 to 10. The default number is 1.

Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the times for which the local AS number can appear.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number cannot appear in routes from the peer/peer group.

Examples

Configure the number of times for which the local AS number can appear in the AS PATH of routes from the peer as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 allow-as-loop 2
```

peer as-path-acl (IPv6 MBGP address family view)

Syntax

peer { *ipv6-address* | *ipv6-group-name* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *ipv6-address* | *ipv6-group-name* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

as-path-acl-number: AS path ACL number, in the range 1 to 256.

import: Filters incoming IPv6 MBGP routes.

export: Filters outgoing IPv6 MBGP routes.

Description

Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to an IPv6 MBGP peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL is specified for filtering the routes from/to an IPv6 MBGP peer/peer group.

Examples

Specify AS path ACL 3 to filter routes outgoing to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 as-path-acl 3 export
```

peer default-route-advertise (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

route-policy-name: Route policy name, a string of 1 to 19 characters.

Description

Use the **peer default-route-advertise** command to advertise a default route to an IPv6 MBGP peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to an IPv6 MBGP peer/peer group.

By default, no default route is advertised to any IPv6 MBGP peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the IPv6 MBGP peer/peer group regardless of whether the default route is available in the routing table.

Examples

Advertise a default route to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 default-route-advertise
```

peer enable (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **enable**

undo peer { *ipv6-group-name* | *ipv6-address* } **enable**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters. The IPv6 MBGP peer group must be created in IPv6 MBGP view before being activated here.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer enable** command to enable an IPv6 MBGP peer or peer group.

Use the **undo peer enable** command to disable an IPv6 MBGP peer or peer group.

By default, no IPv6 MBGP peer or peer group is enabled.

If an IPv6 MBGP peer or peer group is disabled, the router will not exchange routing information with it.

Examples

Enable IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
```

peer filter-policy (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **filter-policy** *acl6-number* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **filter-policy** [*acl6-number*] { **import** | **export** }

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

acl6-number: IPv6 ACL number, in the range 2000 to 3999.

import: Applies the filter to routes received from the IPv6 MBGP peer/peer group.

export: Applies the filter to routes advertised to the IPv6 MBGP peer/peer group.

Description

Use the **peer filter-policy** command to configure an IPv6 ACL-based filter policy for an IPv6 MBGP peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no IPv6 ACL-based filter policy is configured for any IPv6 MBGP peer or peer group.

Examples

Apply IPv6 ACL 2000 to filter routes advertised to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 MBGP address family view)

Syntax

peer *ipv6-address* **group** *ipv6-group-name*

undo peer *ipv6-address* **group** *ipv6-group-name*

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer group** command to add an IPv6 MBGP peer to a configured IPv6 MBGP peer group.

Use the **undo peer group** command to delete a specified IPv6 MBGP peer from an IPv6 MBGP peer group.

By default, no IPv6 MBGP peer is added into any IPv6 MBGP peer group.

Examples

Create an IPv6 MBGP peer group named **test** and add the IPv6 MBGP peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 group test
```

peer ipv6-prefix (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

import: Applies the IPv6 prefix list to filter routes received from the IPv6 MBGP peer/peer group.

export: Applies the IPv6 prefix list to filter routes advertised to the specified IPv6 MBGP peer/peer group.

Description

Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list based filtering is configured.

Examples

Apply the IPv6 ACL **list1** to filter routes advertised to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 ipv6-prefix list1 export
```

peer keep-all-routes (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

undo peer { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a IPv6 MBGP peer.

Description

Use the **peer keep-all-routes** command to save the original routing information from an IPv6 MBGP peer or peer group, including routes that fail to pass the inbound filtering policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the original routing information from an IPv6 MBGP peer or peer group is not saved.

Examples

Save the original routing information from IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 keep-all-routes
```

peer next-hop-local (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

undo peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer next-hop-local** command to configure the next hop of routes advertised to an IPv6 MBGP peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, an IPv6 MBGP speaker specifies itself as the next hop for routes outgoing to an IPv6 multicast eBGP peer/peer group rather than an IPv6 multicast iBGP peer/peer group.

Examples

Set the next hop of routes advertised to iBGP peer group **test** to the advertising router.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test next-hop-local
```

peer preferred-value (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*

undo peer { *ipv6-group-name* | *ipv6-address* } **preferred-value**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

value: Preferred value, in the range 0 to 65535.

Description

Use the **peer preferred-value** command to assign a preferred value to routes received from an IPv6 MBGP peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

The preferred value defaults to 0.

Routes learned from peers each have a preferred value. Among multiple routes to the same destination, the route with the greatest preferred value is selected.

Note the following:

If you both reference a route policy and use the **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value* command to set a preferred value for routes from a peer, the route policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the route policy uses the value set with the **peer preferred-value** command. If the preferred value specified in the route policy is zero, the routes matching it will also use the value set with the command. For information about using a route policy to set a preferred value, refer to the command **peer** { *group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** } in this document, and the command **apply preferred-value** *preferred-value* in *Route Policy Commands* of the *IP Routing Volume*.

Examples

Configure a preferred value of 50 for routes from IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

undo peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer public-as-only** command to disable IPv6 MBGP updates to a peer/peer group from carrying private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 MBGP updates to a peer/peer group to carry private AS numbers.

By default, private AS numbers can be carried in outbound IPv6 MBGP update packets.

The command does not take effect for IPv6 MBGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

Examples

Disable updates sent to IPv6 MBGP peer 1:2::3:4 from carrying private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **reflect-client**

undo peer { *ipv6-group-name* | *ipv6-address* } **reflect-client**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify an IPv6 MBGP peer/peer group as its client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients**, **reflector cluster-id**.

Examples

Configure the local device as a route reflector and specify the peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test reflect-client
```

peer route-limit (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **route-limit** *limit* [*percentage*]

undo peer { *ipv6-group-name* | *ipv6-address* } **route-limit**

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

limit: Specifies the upper limit of IPv6 address prefixes that can be received from the peer or peer group, in the range 1 to 6144.

percentage: If the number of received routes divided by the upper limit reaches the specified percentage, the system will generate alarm information. The percentage is in the range 1 to 100. The default is 75.

Description

Use the **peer route-limit** command to set the maximum number of IPv6 prefixes that can be received from an IPv6 MBGP peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the IPv6 prefixes from an IPv6 MBGP peer/peer group are unlimited.

The router will tear down the TCP connection when the number of IPv6 prefixes received from the peer exceeds the limit.

Examples

Set the number of IPv6 address prefixes allowed to receive from the IPv6 MBGP peer 1:2::3:4 to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 route-limit 10000
```

peer route-policy (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

route-policy-name: Route policy name, a string of 1 to 19 characters.

import: Applies the route-policy to routes received from the IPv6 MBGP peer/peer group.

export: Applies the route-policy to routes advertised to the IPv6 MBGP peer/peer group.

Description

Use the **peer route-policy** command to apply a route policy to routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no route policy is applied to the routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

The **if-match interface** clause in the route policy referenced by the **peer route-policy** command will not be applied.

Refer to *Route Policy Commands* in the *IP Routing Volume* for related information.

Examples

Apply the route policy **test-policy** to routes received from the IPv6 MBGP peer group **test**.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test route-policy test-policy import
```

preference (IPv6 MBGP address family view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

external-preference: Preference of IPv6 multicast eBGP routes, in the range 1 to 255. An IPv6 multicast eBGP route is learned from an IPv6 multicast eBGP peer.

internal-preference: Preference of IPv6 multicast iBGP routes, in the range 1 to 255. An IPv6 multicast iBGP route is learned from an IPv6 multicast iBGP peer.

local-preference: Preference of locally generated IPv6 MBGP routes, in the range 1 to 255.

route-policy-name: Route policy name, a string of 1 to 19 characters. Using a route policy, you can configure the preferences for the routes that match the filtering conditions. As for the unmatched routes, the default preferences are adopted.

Description

Use the **preference** command to configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes.

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

The default preference values of external, internal and local IPv6 MBGP routes are 255, 255, and 130, respectively.

The greater the preference value is, the lower the preference is.

Examples

Configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] preference 20 20 200
```

reflect between-clients (IPv6 MBGP address family view)

Syntax

reflect between-clients

undo reflect between-clients

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to the other clients. If the clients of a route reflector are fully meshed, you need to disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples

Enable route reflection between clients

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
```

```
[Sysname-bgp-af-ipv6-mul] reflect between-clients
```

reflector cluster-id (IPv6 MBGP address family view)

Syntax

reflector cluster-id *cluster-id*

undo reflector cluster-id

View

IPv6 MBGP address family view

Default Level

2: System level

Parameters

cluster-id: Cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a cluster has multiple route reflectors, you need to use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

Examples

Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] reflector cluster-id 50
```

refresh bgp ipv6 multicast

Syntax

refresh bgp ipv6 multicast { *ipv6-address* | **all** | **external** | **group** *ipv6-group-name* | **internal** } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

ipv6-address: Soft-resets the connection to the specified IPv6 MBGP peer.

all: Soft-resets all IPv6 MBGP connections.

external: Soft-resets IPv6 multicast eBGP connections.

group *ipv6-group-name*: Soft-resets connections to an IPv6 multicast peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IPv6 multicast iBGP connections.

export: Performs soft-reset in outbound direction.

import: Performs soft-reset in inbound direction.

Description

Use the **refresh bgp ipv6 multicast** command to soft-reset specified IPv6 MBGP connections. With this feature, you can refresh the IPv6 MBGP routing table and apply a new policy without tearing down IPv6 MBGP connections.

To perform IPv6 MBGP soft-reset, all routers in the network should support route-refresh. If a peer not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates from the peer before performing soft reset.

Examples

Soft-reset inbound IPv6 MBGP connections.

```
<Sysname> refresh bgp ipv6 multicast all import
```

reset bgp ipv6 multicast

Syntax

reset bgp ipv6 multicast { *as-number* | *ipv6-address* | **all** | **group** *ipv6-group-name* | **external** | **internal** }

View

User view

Default Level

2: System level

Parameters

as-number: Resets the connections to IPv6 MBGP peers in the specified AS.

ipv6-address: Resets the connection to the specified peer.

flap-info: Clears routing flap information.

all: Resets all IPv6 MBGP connections.

group *ipv6-group-name*: Resets the connections to the specified IPv6 MBGP peer group.

external: Resets all the IPv6 multicast eBGP connections.

internal: Resets all the IPv6 multicast iBGP connections.

Description

Use the **reset bgp ipv6 multicast** command to reset specified IPv6 MBGP connections to reconnect to the peers.

Examples

Reset all the IPv6 MBGP connections.

```
<Sysname> reset bgp ipv6 multicast all
```

reset bgp ipv6 multicast dampening

Syntax

reset bgp ipv6 multicast dampening [*ipv6-address prefix-length*]

View

User view

Default Level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address..

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

Description

Use the **reset bgp ipv6 multicast dampening** command to clear route dampening information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all IPv6 MBGP route dampening information will be cleared.

Examples

Clear the damping information of the route 2345::/64 and release the suppressed route.

```
<Sysname> reset bgp ipv6 multicast dampening 2345::64
```

reset bgp ipv6 multicast flap-info

Syntax

reset bgp ipv6 multicast flap-info [*ipv6-address/prefix-length* | **regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number*]

View

User view

Default Level

1: Monitor level

Parameters

ipv6-address: Clears the routing flap statistics for the specified IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 1 to 128.

as-path-regexp: Clears the routing flap statistics for routes matching the AS path regular expression.

as-path-acl-number: Clears the routing flap statistics for routes matching the AS path ACL. The value of this argument is in the range of 1 to 256.

Description

Use the **reset bgp ipv6 multicast flap-info** command to clear IPv6 MBGP routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples

Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp ipv6 multicast flap-info as-path-acl 10
```

Table of Contents

1 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 the MLD Snooping multicast group information for the specified card. If you do not specify a slot, this command will display the MLD Snooping multicast group information on the SRPU.

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.
```

```
        Eth2/0/1                (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.
        Eth2/0/2                (D) ( 00:03:23 )
MAC group(s):
    MAC group address:3333-0000-0101
      Host port(s):total 1 port.
        Eth2/0/2
```

Table 1-1 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. On a distributed device, to get this time value of a non-aggregation port that does not belong to the SRPU, you must specify the number of the slot where the corresponding board resides; this is not required on an aggregation port.
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 1-2 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

drop-unknown (MLD-Snooping view)

Syntax

drop-unknown

undo drop-unknown

View

MLD-Snooping view

Default Level

2: System level

Parameters

None

Description

Use the **drop-unknown** command to enable dropping unknown IPv6 multicast data globally.

Use the **undo drop-unknown** command to disable dropping unknown IPv6 multicast data globally.

By default, this function is disabled, that is, unknown IPv6 multicast data is flooded in the VLAN.

This command works only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

Related commands: **mld-snooping drop-unknown**.

Examples

Globally enable the device to drop unknown IPv6 multicast data.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] drop-unknown
```

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.

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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- 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.

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.

```
<Sysname> system-view
[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 only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

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 only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

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 only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

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 drop-unknown

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping drop-unknown** command to enable dropping unknown IPv6 multicast data in the current VLAN.

Use the **undo mld-snooping drop-unknown** command to disable dropping unknown IPv6 multicast data in the current VLAN.

By default, this function is disabled, unknown IPv6 multicast data is flooded in the VLAN.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **drop-unknown**.

Examples

Enable dropping unknown IPv6 multicast data in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping drop-unknown
```

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 interface view, Layer 2 aggregate interface 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.

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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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 512.

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 512.

Note that:

- You can also use the mld group-limit command to limit the number of IPv6 multicast groups that can be joined on an port. If you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for the VLAN interface, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of groups only on the VLAN interface.
- If you do not specify any VLAN when using this command in Ethernet porti 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: **mld group-limit** in *MLD Commands* in the *IP Multicast Volume*.

Examples

Specify to allow a maximum of 10 IPv6 multicast groups to be joined on Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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).

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 interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 on Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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) 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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces, and the version of MLD on the simulated host depends on the version of MLD Snooping running in the VLAN or the version of MLD running on the VLAN interface.
- 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 interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 2/0/1 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 ethernet2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface 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.

This command works on both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

Examples

Enable source port filtering for IPv6 multicast data on Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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 interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 2/0/1 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 interface view, Layer 2 aggregate interface 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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.
- If configured in Ethernet interface view or Layer 2 aggregate interface view, this feature takes effect only if the interface 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 Ethernet 2/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- 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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

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 only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.
- 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 only on MLD Snooping–enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

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 both MLD Snooping–enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

Examples

Enable source port filtering for IPv6 multicast data on interfaces Ethernet 2/0/1 through Ethernet 2/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port ethernet 2/0/1 to ethernet 2/0/4
```

Table of Contents

1 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 4 IPv6 multicast-vlan(s)
 IPv6 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port
 IPv6 Multicast vlan 200
   subvlan list:
    no subvlan
   port list:
    GE2/0/1                 GE2/0/2
 IPv6 Multicast vlan 300
   subvlan list:
    vlan 3
   port list:
    GE2/0/3                 GE2/0/4
 IPv6 Multicast vlan 400
```

```
subvlan list:
 no subvlan
port list:
 no port
```

Table 1-1 display multicast-vlan ipv6 command output description

Field	Description
Total 4 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.
- The IPv6 multicast VLAN feature cannot be enabled on a device with IPv6 multicast routing enabled.
- 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: **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*; **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 interfaces can be configured as IPv6 multicast VLAN ports: Ethernet, and Layer 2 aggregate interfaces.

Examples

Assign ports GigabitEthernet 2/0/1 through GigabitEthernet 2/0/5 to IPv6 multicast VLAN 100.

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

```
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] port gigabitethernet 2/0/1 to gigabitethernet 2/0/5
```

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 IPv6 multicast VLAN must not exceed the system-defined limit (an S7900E series Ethernet switch supports up to five multicast VLANs, and supports up to 4000 sub-VLANs for each multicast VLAN. The total number of sub-VLANs for all multicast VLANs on the switch cannot exceed 4000.).

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
```

MPLS Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The MPLS Volume is organized as follows:

Features	Description
MCE	Multi-CE (MCE) enables a switch to function as the CEs of multiple VPN instances in a BGP/MPLS VPN network, thus reducing the investment on network equipment. This document introduces the commands for MCE configuration.
MPLS Basics	MPLS (Multiprotocol Label Switching) brings together the advantages of the connectionless control with IP and the connection-oriented forwarding with ATM. In addition to the support from IP routing and control protocols, its powerful and flexible routing functions allows it to accommodate to various emerging applications. This document introduces the commands for MPLS Basics configuration.
MPLS L2VPN	MPLS L2VPN provides Layer 2 VPN services on the MPLS network. This document introduces the commands for MPLS L2VPN configuration.
MPLS L3VPN	MPLS L3VPN is a kind of PE-based L3VPN technology for service provider VPN solutions. This document introduces the commands for MPLS L3VPN configuration.

Table of Contents

1 MCE Configuration Commands

Note

This chapter only describes the commands related to the multi-CE (MCE) feature. For information about the routing protocol configuration commands in the configuration examples, refer to the *IP Routing Volume* of this manual.

MCE Configuration Commands

description

Syntax

description *text*

undo description

View

VPN instance view

Default Level

2: System level

Parameters

text: Description for the VPN instance, a string of 1 to 80 characters.

Description

Use the **description** command to configure a description for the current VPN instance.

Use the **undo description** command to delete the description.

Examples

Configure the description of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] description vpn1
```

display bgp vpnv4 vpn-instance group

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **group** [*group-name*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of the BGP peer group, a string of 1 to 47 characters.

Description

Use the **display bgp vpnv4 group** command display information about a specified or all BGP VPNv4 peer group.

Examples

Display information about BGP VPNv4 peer group a for VPN instance vpn1.

```
BGP peer-group is a
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 99
 No routing policy is configured
  Members:
 Peer        V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State
 10.1.1.1    4   200   18       21     0     1      00:12:58 Established
```

Table 1-1 Description on the fields of the **display bgp vpnv4 group** command

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS number	Number of the remote AS
Type	Peer group type
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Configured hold timer value	Setting of the hold timer
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum route advertisement interval
Peer Preferred Value	Weight for the routes from the peer
No routing policy is configured	Whether the VPN instance is configured with a routing policy
Peer	IP address of the peer

Field	Description
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

display bgp vpnv4 vpn-instance network

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **network**

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of a VPN instance, a string of 1 to 31 characters.

Description

Use the **display bgp vpnv4 network** command to display information about BGP VPNv4 routes injected into a specified or all VPN instances.

Examples

Display information about BGP VPNv4 routes injected into VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 network
  BGP Local Router ID is 1.1.1.1.
  Local AS Number is 100.
  Network          Mask            Route-policy
  10.0.0.0         255.0.0.0
```

Table 1-2 Description on the fields of the **display bgp vpnv4 network** command

Field	Description
BGP Local Router ID	Router ID of the local BGP router
Local AS Number	Local AS number
Network	Advertised network route
Mask	Mask of the advertised network route

Field	Description
Route-policy	Routing policy configured

display bgp vpnv4 vpn-instance paths

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **paths** [*as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

as-regular-expression: Regular expression for filtering the AS path information to be displayed.

Description

Use the **display bgp vpnv4 paths** command to display the BGP VPNv4 AS path information.

Examples

Display the BGP VPNv4 AS path information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 paths

    Address       Hash    Refcount  MED         Path/Origin
    0x6E72D18     0       1           0           200?
    0x6E72E50     0       1           0           i
    0x6E72B78     1       1           0           ?
0x6E72BE0     1       2           0           ?
```

Table 1-3 Description on the fields of the **display bgp vpnv4 paths** command

Field	Description
Address	Routing address in the local database
Hash	Hash bucket for storing routes
Refcount	Number of times that the path is referenced
MED	Metric for routes
Path/Origin	AS_PATH attribute/Route origin code

display bgp vpnv4 vpn-instance peer

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **peer** [*group-name* **log-info** | *ip-address* { **log-info** | **verbose** } | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of a peer group, a string of 1 to 47 characters.

log-info: Displays the log information about the peer group.

ip-address: IP address of the peer.

verbose: Displays detailed information.

Description

Use the **display bgp vpnv4 peer** command to display information about BGP VPNv4 peers.

Examples

Display information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer

 BGP local router ID : 2.2.2.2
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1
 Peer       V    AS  MsgRcvd  MsgSent  OutQ   PrefRcv   Up/Down        State

 10.1.1.1  4   200         24       29      0          1  00:18:47 Established
```

Table 1-4 Description on the fields of display bgp vpnv4 vpn-instance peer

Field	Description
BGP Local router ID	Router ID of the local BGP router
local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in the state of established
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received

Field	Description
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of received prefixes
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer verbose

         Peer: 10.1.1.1  Local: 2.2.2.2
         Type: EBGP link
         BGP version 4, remote router ID 10.1.1.1
         BGP current state: Established, Up for 00h19m26s
         BGP current event: KATimerExpired
         BGP last state: OpenConfirm
         Port:  Local - 179      Remote - 1025
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer support bgp multi-protocol extended
         Peer support bgp route refresh capability
         Address family IPv4 Unicast: advertised and received

 Received: Total 25 messages, Update messages 1
 Sent: Total 30 messages, Update messages 4
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 Nesting-vpn peer (vpn-instance vrf1) has been configured
 Peer Preferred Value: 99

 Routing policy configured:
 No routing policy is configured
```

Table 1-5 Description on the fields of the **display bgp vpnv4 peer verbose** command

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs

Field	Description
remote router ID	Router ID of the remote router
BGP current state	Current status of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current status
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Received	Total number of received messages and the number of received update messages
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Local optional capabilities
Route refresh capability has been enabled	Whether the route refresh capability is supported
Nesting-vpn peer	Whether the VPNv4 peer is a nested VPN peer
Peer Preferred Value	Weight for the routes from the peer
Routing policy configured	Routing policy configured

display bgp vpnv4 vpn-instance routing-table

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table** [*network-address* [{ *mask-length* | *mask-address* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13>[**no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **dampened** | **dampening parameter** | **different-origin-as** | **flap-info** [**as-path-acl** *as-path-acl-number* | *network-address* [*mask* [**longer-match**] | *mask-length*

[**longer-match**]] | **regular-expression** *as-regular-expression*] | **peer** *ip-address* { **advertised-routes** | **received-routes** } | **regular-expression** *as-regular-expression* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

network-address: IP address of the destination segment.

mask-length: Length of the network mask, in the range 0 to 32.

mask-address: Network mask, in the format of X.X.X.X.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays classless interdomain routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

dampened: Displays information about dampened BGP VPNv4 routes.

dampening parameter: Configured BGP VPNv4 route dampening parameters.

different-origin-as: Displays information about routes with different AS origins.

flap-info: Displays BGP VPNv4 route flap statistics.

longer-match: Displays flap statistics for routes with greater mask lengths than that specified by the *network-address* { *mask* | *mask-length* } combination.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Displays routing information sent to the specified peer.

received-routes: Displays routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

statistic: Displays BGP VPNv4 route statistics.

Description

Use the **display bgp vpnv4 vpn-instance routing-table** command to display the BGP VPNv4 routing information of a specified VPN instance.

Examples

Display the BGP VPNv4 routing information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 routing-table
 Total Number of Routes: 5

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Network            NextHop         MED        LocPrf    PrefVal Path/Ogn

 *>i 10.0.0.0       1.1.1.1         0          100         0       i
 *>  10.1.1.0/24    0.0.0.0         0                       0       ?
 *>  20.0.0.0       10.1.1.1        0                       99      200?
 *>i 123.1.1.1/32   1.1.1.1         0          100         0       ?
 *>  124.1.1.1/32   0.0.0.0         0                       0       ?
```

Table 1-6 Description on the fields of display bgp vpnv4 vpn-instance routing-table

Field	Description
Total Number of Routes	Total number of routes
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status code. For valid values.
Origin	Route origin code. For valid values.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
MED	Metric associated with the destination network
LocPrf	Local preference
PrefVal	Preferred value of the protocol
Path/Ogn	AS_PATH attribute/Route origin code.

display fib vpn-instance

Syntax

display fib vpn-instance *vpn-instance-name* [**include** *string*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

include: Displays the lines that include the specified string.

string: String for matching against the information to be displayed. It is case sensitive and consists of 1 to 256 characters.

Description

Use the **display fib vpn-instance** command to display the FIB information of a VPN instance.

Examples

Display all FIB information of VPN instance **vpn1**.

```
<Sysname> display fib vpn-instance vpn1
<Sysname> display fib vpn-instance vpn1
FIB Table For vpn1:
 Total number of Routes : 2
Destination/Mask    OutInterface                 InnerLabel     Token
66.1.1.1/32         InLoopBack0                  NULL           invalid
66.1.1.0/24         InLoopBack0                  NULL           invalid
```

Table 1-7 display fib vpn-instance command output description

Field	Description
FIB entry count	Number of entries in the FIB
Destination/Mask	Destination address/mask length
OutInterface	Forwarding interface
Token	LSP index number

display ip routing-table vpn-instance

Syntax

display ip routing-table vpn-instance *vpn-instance-name* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

verbose: Displays detailed information.

Description

Use the **display ip routing-table vpn-instance** command to display the routing information of a VPN instance.

Examples

Display the routing information of VPN instance vpn2.

```
<Sysname> display ip routing-table vpn-instance vpn2
Routing Tables: vpn2
         Destinations : 5        Routes : 5

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
10.214.20.0/24      Direct 0    0            10.214.20.3     Vlan20
10.214.20.3/32      Direct 0    0            127.0.0.1       InLoop0
192.168.10.0/24     RIP    100  1            10.214.20.2     Vlan20
```

Table 1-8 Description on the fields of display ip routing-table vpn-instance

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol discovering the route
Pre	Preference of the route
Cost	Cost of the route
NextHop	Address of the next hop along the route
Interface	Outbound interface for forwarding packets to the destination segment

display ip vpn-instance

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description

Use the **display ip vpn-instance** command to display information about a VPN instance or all VPN instances.

If you do not specify any parameter, the command displays brief information about all VPN instances.

Examples

Display information about all VPN instances.

```
<Sysname> display ip vpn-instance
  Total VPN-Instances configured : 2

  VPN-Instance Name      RD          Create Time
  vpn1                   22:1        2003/10/13 09:32:45
  vpn2                   33:3        2003/10/13 09:42:59
```

Table 1-9 Description on the fields of the **display ip vpn-instance** command

Field	Description
VPN-Instance Name	Name of the VPN instance
RD	RD of the VPN instance
Create Time	Time when the VPN instance was created

Display detailed information about a specified VPN instance.

```
<Sysname> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and ID : vpn1, 1
  Create time : 2006/04/08 13:01:30
  Up time : 0 days, 00 hours, 11 minutes and 42 seconds
  Route Distinguisher : 22:1
  Export VPN Targets :  3:3 5:5
  Import VPN Targets :  4:4 5:5
  Import Route Policy : poly-1
  Description : This is vpn1
  Maximum number of Routes : 500
  Interfaces :  Vlan-interface10
```

Table 1-10 Description on the fields of display ip vpn-instance instance-name

Field	Description
VPN-Instance Name and ID	Name and ID of the VPN instance
CreateTime	Time when the VPN instance was created
Up time	Duration of the VPN instance
Route Distinguisher	RD of the VPN instance
Export VPN Targets	Export target attribute of the VPN instance

Field	Description
Import VPN Targets	Import target attribute of the VPN instance
Import Route Policy	Import routing policy of the VPN instance
Description	Description of the VPN instance
Maximum number of Routes	Maximum number of routes of the VPN instance
Interfaces	Interface to which the VPN instance is bound

domain-id

Syntax

domain-id *domain-id* [**secondary**]

undo domain-id [*domain-id*]

View

OSPF view

Default Level

2: System level

Parameters

domain-id: OSPF domain ID, in integer or dotted decimal notation. If it is in integer, it ranges from 0 to 4,294,967,295.

secondary: Uses the domain ID as secondary. With this keyword not specified, the domain ID configured is primary.

Description

Use the **domain-id** command to configure an OSPF domain ID.

Use the **undo domain-id** command to restore the default.

By default, the OSPF domain ID is 0.

With no parameter specified, the **undo domain-id** command deletes all domain IDs.

Usually, routes injected from PEs are advertised as External-LSAs. However, routes to different destinations in the same OSPF domain must be advertised as Type-3 LSAs. Therefore, using the same domain ID is required for an OSPF domain.

Examples

Configure the OSPF domain ID.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpn1
[Sysname-ospf-100] domain-id 234
```

export route-policy

Syntax

export route-policy *route-policy*

undo export route-policy

View

VPN instance view

Default Level

2: System level

Parameters

route-policy: Name of the export routing policy for the VPN instance, a string of 1 to 19 characters.

Description

Use the **export route-policy** command to apply an export routing policy to a VPN instance.

Use the **undo export route-policy** command to remove the application.

You can configure an export routing policy when a finer control on the VPN instance routes to be redistributed is required, that is, when the control provided by the extended community attribute is not enough. An export routing policy may deny routes that are permitted by the export target attribute.

By default, all VPN instance routes permitted by the export target attribute can be redistributed.

Examples

Apply export routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

ext-community-type

Syntax

ext-community-type { **domain-id** *type-code1* | **router-id** *type-code2* | **route-type** *type-code3* }

undo ext-community-type { **domain-id** | **router-id** | **route-type** }

View

OSPF view

Default Level

2: System level

Parameters

domain-id *type-code1*: Specifies the type code for the OSPF extended community attribute of Domain ID. Valid values are 0x0005, 0x0105, 0x0205, and 0x8005.

router-id *type-code2*: Specifies the type code for the OSPF extended community attribute of Router ID. Valid values are 0x0107 and 0x8001.

route-type *type-code3*: Specifies the type code for the OSPF extended community attribute of Route Type. Valid values are 0x0306 and 0x8000.

Description

Use the **ext-community-type** command to configure the type code of an OSPF extended community attribute.

Use the **undo ext-community-type** command to restore the default.

By default, the type codes for the OSPF extended community attributes of Domain ID, Router ID, and Route Type are 0x0005, 0x0107, and 0x0306 respectively.

Examples

Configure the type codes of OSPF extended community attributes Domain ID, Router ID, and Route Type as 0x8005, 0x8001, and 0x8000 respectively for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ext-communityroute-type domain-id 8005
[Sysname-ospf-100] ext-communityroute-type router-id 8001
[Sysname-ospf-100] ext-communityroute-type route-type 8000
```

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View

BGP-VPN instance view

Default Level

2: System level

Parameters

acl-number: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

direct: Filters direct routes to be advertised.

isis *process-id*: Filters ISIS routes to be advertised that are from a specified ISIS process. The *process-id* argument is in the range 1 to 4294967295.

ospf *process-id*: Filters OSPF routes to be advertised that are from a specified OSPF process. The *process-id* argument is in the range 1 to 4294967295.

rip *process-id*: Filters RIP routes to be advertised that are from a specified RIP process. The *process-id* argument is in the range 1 to 4294967295.

static: Filters static routes to be advertised.

Description

Use the **filter-policy export** command to configure BGP to filter all or certain types of routes to be advertised.

Use the **undo filter-policy export** command to remove the configuration.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised will be filtered.

By default, BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by BGP.

Examples

Configure BGP to filter the routes to be advertised by using ACL 2555.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2555 export
```

filter-policy import

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View

BGP-VPN instance view

Default Level

2: System level

Parameters

acl-number: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to configure BGP to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

By default, BGP does not filter received routes.

Only routes that survive the filtering are added into the BGP routing table.

Examples

Configure BGP to filter received routes using ACL 2255.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2255 import
```

import route-policy

Syntax

import route-policy *route-policy*

undo import route-policy

View

VPN instance view

Default Level

2: System level

Parameters

route-policy: Name of the import routing policy for the VPN instance, a string of 1 to 19 characters.

Description

Use the **import route-policy** command to apply an import routing policy to a VPN instance.

Use the **undo import route-policy** command to remove the application.

You can configure an import routing policy when a finer control on the routes to be redistributed into a VPN instance is required, that is, when the control provided by the extended community attributes is not enough. An import routing policy may deny routes that are permitted by the import target attributes.

By default, all routes permitted by the import target attribute can be redistributed into the VPN instance.

Examples

Apply import routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1
```

ip binding vpn-instance

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

View

Interface view

Default Level

2: System level

Parameters

vpn-instance-name: Name of the VPN instance to be associated, a case-insensitive string of 1 to 31 characters.

Description

Use the **ip binding vpn-instance** command to associate an interface with a VPN instance.

Use the **undo ip binding vpn-instance** command to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must re-configure the IP address of the interface after configuring the command.

Examples

Associate Vlan-interface 1 with the VPN instance named “vpn1”.

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1
```

ip vpn-instance

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

View

System view

Default Level

2: System level

Parameters

vpn-instance-name: Name of the VPN instance, a case-insensitive string of 1 to 31 characters.

Description

Use the **ip vpn-instance** command to create a VPN instance and enter VPN instance view.

Use the **undo ip vpn-instance** command to delete a VPN instance.

A VPN instance takes effect only after you configure an RD for it.

Related command: **route-distinguisher**.

Examples

Create a VPN instance named vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

ipv4-family vpn-instance

Syntax

ipv4-family vpn-instance *vpn-instance-name*

undo ipv4-family vpn-instance *vpn-instance-name*

View

BGP view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Associates a VPN instance with an IPv4 address family and enters BGP VPN instance view. The *vpn-instance-name* argument is a string of 1 to 31 characters.

Description

Use the **ipv4-family** command to enter BGP-VPN instance view.

Use the **undo ipv4-family** command to remove all the configurations performed in either of the two views.

Before entering BGP VPN instance view, make sure the corresponding VPN instance is created.

Examples

Enter BGP-VPN instance view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1]
```

peer allow-as-loop

Syntax

peer { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View

BGP-VPN instance view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

number: Maximum number that the local AS number can appear repeatedly in the AS-PATH attribute. It ranges from 1 to 10 and defaults to 1.

Description

Use the **peer allow-as-loop** command to allow the local AS number to appear in the AS-PATH attribute of a received route and to set the allowed maximum number of repetitions.

Use the **undo peer allow-as-loop** command to remove the configuration.

Examples

Allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

peer group

Syntax

peer *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View

BGP-VPN instance view

Default Level

2: System level

Parameters

ip-address: IP address of a peer.

group-name: Name of a peer group, a string of 1 to 47 characters.

as-number *as-number*: Specifies an AS number, which ranges from 1 to 65535.

Description

Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to remove a peer from a peer group.

Examples

Add the peer with the IP address 1.1.1.1 to the peer group named “test”.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 group test
```

refresh bgp vpn-instance

Syntax

refresh bgp vpn-instance *vpn-instance-name* { *ip-address* | **all** | **external** | **group** *group-name* } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of a VPN instance, a string of 1 to 31 characters.

ip-address: IP address of a peer.

all: Performs a soft reset of all BGP VPN instance connections.

external: Performs a soft reset of EBGP sessions.

group *group-name*: Performs a soft reset of the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description

Use the **refresh bgp vpn-instance** command to perform a soft reset of BGP connections in a VPN instance.

Examples

Perform a soft reset of all BGP connections in VPN instance vpn1 in the inbound direction to make new configurations take effect.

```
<Sysname> refresh bgp vpn-instance vpn1 all import
```

reset bgp vpn-instance

Syntax

reset bgp vpn-instance *vpn-instance-name* { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* }

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of a VPN instance, a string of 1 to 31 characters.

as-number: AS number, in the range 1 to 4294967295.

ip-address: IP address of a peer.

group *group-name*: Resets the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

all: Resets all BGP connections.

external: Resets EBGP sessions.

Description

Use the **reset bgp vpn-instance** command to reset the BGP connections of a specified VPN instance.

Examples

Reset all BGP connections of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 all
```

reset bgp vpn-instance dampening

Syntax

reset bgp vpn-instance *vpn-instance-name* **dampening** [*network-address* [*mask* | *mask-length*]]

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

dampening: Specifies route flap dampening information.

network-address: Network address.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

Description

Use the **reset bgp vpn-instance dampening** command to clear the route flap dampening information of a VPN instance.

Examples

Clear the route flap dampening information of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 dampening
```

reset bgp vpn-instance flap-info

Syntax

reset bgp vpn-instance *vpn-instance-name ip-address* **flap-info**

reset bgp vpn-instance *vpn-instance-name* **flap-info** [*ip-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **regexp** *as-path-regexp*]

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: IP address of the peer.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

as-path-acl *as-path-acl-number*: Specifies the AS_PATH filtering list. The *as-path-acl-number* argument ranges from 1 to 256.

regexp *as-path-regexp*: Specifies the AS_PATH regular expression.

Description

Use the **reset bgp vpn-instance flap-info** command to clear the route flap history information about BGP peers of a VPN instance.

Examples

Clear route flap history information about BGP peer 2.2.2.2 of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 2.2.2.2 flap-info
```

route-distinguisher

Syntax

route-distinguisher *route-distinguisher*

View

VPN instance view

Default Level

2: System level

Parameters

route-distinguisher: Route distinguisher (RD) for the VPN instance, a string of 3 to 21 characters in either of the following two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

Description

Use the **route-distinguisher** command to configure a route distinguisher (RD) for a VPN instance.

An RD is used to create the routing and forwarding table of a VPN. By prefixing an RD to an IPv4 prefix, you make the VPN IPv4 prefix unique globally.

Note

- No RD is configured by default; you must configure an RD for each VPN instance.
- A VPN instance takes effect only after you configure an RD for it.
- Once you configure an RD for a VPN, you cannot remove the association.
- You cannot change an RD directly; you can only delete the VPN instance, re-create the VPN instance, and then re-configure a new RD.

Examples

Configure the RD of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

routing-table limit

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

View

VPN instance view

Default Level

2: System level

Parameters

number: Maximum number of routes for the VPN instance to support, in the range 1 to 128000.

warn-threshold: Threshold for warning. It is expressed in the maximum percentage of the number of routes for the VPN instance. It ranges from 1 to 100. When the specified threshold is reached, the system gives an alarm message but still allows new routes. If the number of routes received reaches the maximum supported, no more routes will be activated..

simply-alert: Specifies that when the maximum number of routes exceeds the threshold, the system still accepts routes and generates only a SYSLOG error message.

Description

Use the **routing-table limit** command to limit the maximum number of routes in a VPN instance, preventing too many routes from being redistributed from the inbound interface of the PE.

Use he **undo routing-table limit** command to remove the limitation.

By default, there is no limit to the maximum number of routes that a VPN instance supports.

Examples

Specify that VPN instance vpn1 can redistribute up to 1000 routes in, and allow the VPN instance to accept new routes after the threshold is exceeded.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

vpn-instance-capability simple

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

View

OSPF multi-instance view

Default Level

2: System level

Parameters

None

Description

Use the **vpn-instance-capability simple** command to enable multi-VPN-instance of OSPF.

Use the **undo vpn-instance-capability** command to disable the function.

By default, the function is disabled.

Examples

Enable multi-VPN-instance of OSPF.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpna
[Sysname-ospf-100] vpn-instance-capability simple
```

vpn-target

Syntax

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | { *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } }

View

VPN instance view

Default Level

2: System level

Parameters

vpn-target&<1-8>: Adds the VPN target extended community attribute to the import or export VPN target extended community list and specify the VPN target in the format nn:nn or IP-address:nn. &<1-8> means that you can specify this argument for up to 8 times.

A VPN target attribute can be of 3 to 21 characters and in either of these two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

both: Specifies both the export routing information to the destination VPN extended community and the import routing information from the destination VPN extended community. This is the default.

export-extcommunity: Specifies the export routing information to the destination VPN extended community.

import-extcommunity: Specifies the import routing information from the destination VPN extended community.

all: Specifies all export routing information to the destination VPN extended community and import routing information from the destination VPN extended community.

Description

Use the **vpn-target** command to associate the current VPN instance with one or more VPN targets.

Use the **undo vpn-target** command to remove the association of the current VPN instance with VPN targets.

VPN target has no default. You must configure it when creating a VPN instance.

Examples

Associate the current VPN instance with VPN targets.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
 EVT Assignment result:
 VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
 IVT Assignment result:
 VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
 IVT Assignment result:
 VPN-Target assignment is successful
 EVT Assignment result:
 VPN-Target assignment is successful
```

Table of Contents

1 MPLS Basics Configuration Commands

Note

- Currently, only VLAN interface supports MPLS capability and LDP capability.
- Except for the command for the LDP GR feature, all commands in MPLS LDP view are available in MPLS LDP VPN instance view. The difference is that the commands serves the public network LDP in MPLS LDP view but serves the MPLS LDP VPN instance in MPLS LDP VPN instance view.
- For information about GR commands, refer to *GR Commands* in the *System Volume*.

MPLS Basic Configuration Commands

display mpls ilm

Syntax

display mpls ilm [*label*] [**slot** *slot-number*] [**include** *text*]

View

Any view

Default Level

1: Monitor level

Parameters

label: Incoming label, in the range 16 to 4294967295.

include *text*: Specifies incoming label mapping (ILM) entries containing a specified string.

slot *slot-number*: Specifies the ILM entries of the board in a slot.

Description

Use the **display mpls ilm** command to display information about ILM entries.

With no incoming label specified, the command displays the ILM entries of all incoming labels.

Examples

Display the ILM entry with a specified incoming label.

```
<Sysname> display mpls ilm 1024
Inlabel In-Interface        Token   VRF-Index Oper   LSP-Type      Swap-Label
------------------------------------------------------------------------------
1024    Vlan2               2         0       POP    NORMAL        ----
```

Display all ILM entries.

```
<Sysname> display mpls ilm
Inlabel In-Interface        Token   VRF-Index Oper   LSP-Type      Swap-Label
------------------------------------------------------------------------------
1024    Vlan2               2         0       POP    NORMAL        ----
```

Table 1-1 display mpls ilm command output description

Field	Description
Inlabel	Incoming label
In-Interface	Incoming interface
Token	NHLFE entry index
VRF-Index	VRF index
Oper	Operation type
LSP-Type	LSP type
Swap-Label	Label for swapping

display mpls interface

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

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

verbose: Displays detailed information.

Description

Use the **display mpls interface** command to display information about one or all interfaces with MPLS enabled.

Related commands: **display mpls statistics interface**, **mpls**.

Examples

Display information about all interfaces with MPLS enabled.

```
<Sysname> display mpls interface
Interface   Status     TE Attr    LSP Count   CRLSP Count
Vlan1         Up         En         0           0
Vlan2         Up         En         0           0
```

Display detailed information about MPLS-enabled interface Vlan-interface 2.

```
<Sysname> display mpls interface vlan-interface 2 verbose
No             : 1
Interface      : Vlan2
Status         : Down
TE Attribute   : Disable
LSPCount       : 0
CR-LSPCount    : 0
FRR            : Disabled
```

Table 1-2 display mpls interface command output description

Field	Description
TE Attr/TE Attribute	Whether TE is enabled on the interface
LSPCount	Number of LSPs on the interface
CR-LSPCount	Number of CR-LSPs on the interface
FRR	Whether FRR is enabled on the interface. If FRR is enabled, the output will also include the bound tunnels.

display mpls label

Syntax

display mpls label { *label-value1* [**to** *label-value2*] | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

label-value1: Specifies a label or, when used with the *label-value2* argument, the start label of a range of labels. The value of this argument ranges from 16 to 8191.

to *label-value2*: Specifies the end label of a range of labels, in the range 16 to 8191.

all: Specifies all labels.

Description

Use the **display mpls label** command to display information about specified labels or all labels.

Examples

Display information about labels in the range 900 to 1500.

```
<Sysname> display mpls label 900 to 1500
Label alloc state: '.' means not used, '$' means used
------------------------------Static Label--------------------------------
900:........ ........ ........ ........  ........ ........ ........ ........
964:........ ........ ........ ........  ........ ........ ........ ....
------------------------------Dynamic Label-------------------------------
```

```
1024:...$.... ........ ........ ........  ........ ........ ........ ........
1088:........ ........ ........ ........  ........ ........ ........ ........
1152:........ ........ ........ ........  ........ ........ ........ ........
1216:........ ........ ........ ........  ........ ........ ........ ........
1280:........ ........ ........ ........  ........ ........ ........ ........
1344:........ ........ ........ ........  ........ ........ ........ ........
1408:........ ........ ........ ........  ........ ........ ........ ........
1472:........ ........ ........ .....
```

display mpls ldp

Syntax

display mpls ldp [**all** [**verbose**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all information about LDP .

verbose: Displays detailed information.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp** command to display information about LDP.

If you do not specify any parameter, the command will display all information about LDP in detail.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Display all information about LDP in detail.

```
<Sysname> display mpls ldp all verbose
                          LDP Global Information
------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 60 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 60 Sec
 MTU Signaling           : Off           Recovery Timer       : 60 Sec

                         LDP Instance Information
```

```
-------------------------------------------------------------
Instance ID            : 0          VPN-Instance         :
Instance Status        : Active     LSR ID               : 1.1.1.1
Hop Count Limit        : 32         Path Vector Limit    : 32
Loop Detection         : Off
DU Re-advertise Timer  : 30 Sec     DU Re-advertise Flag : On
DU Explicit Request    : Off        Request Retry Flag   : On
Label Distribution Mode: Ordered    Label Retention Mode : Liberal
-------------------------------------------------------------
```

Table 1-3 display mpls ldp command output description

Field	Description
Protocol Version	Version of the LDP protocol
Neighbor Liveness	Setting of the GR neighbor liveness timer
Graceful Restart	Whether GR is enabled
FT Reconnect Timer	Setting of the GR's FT reconnect timer
Recovery Timer	Setting of the GR's recovery timer
MTU Signaling	Whether MTU signaling is supported. Currently, the device does not support MTU signaling.
Instance ID	Sequence number of the LDP instance
VPN-Instance	Name of the LDP-enabled VPN instance. For the default instance, nothing is displayed.
Hop Count Limit	Maximum hop count
Path Vector Limit	Maximum path vector length
Loop Detection	Whether loop detection is enabled
DU Re-advertise Flag	Whether label readvertisement is enabled for DU mode
DU Re-advertise Timer	Label readvertisement timer for DU mode
Request Retry Flag	Whether request retransmission is enabled
DU Explicit Request	Whether explicit request transmission is enabled for DU mode
Label Retention Mode	Label retention mode of the instance
Label Distribution Mode	Label distribution mode of the instance

display mpls ldp interface

Syntax

display mpls ldp interface [**all** [**verbose**] | [**vpn-instance** *vpn-instance-name*] [*interface-type interface-number* | **verbose**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all information.

verbose: Displays detailed information.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

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

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp interface** command to display information about LDP-enabled interfaces.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Display information about all LDP-enabled interfaces.

```
<Sysname> display mpls ldp interface
     LDP Interface Information in Public Network
------------------------------------------------------------------------------
 IF-Name         Status       LAM   Transport-Address   Hello-Sent/Rcv
------------------------------------------------------------------------------
 Vlan2           Inactive     DU    1.1.1.1             0/0
------------------------------------------------------------------------------
 LAM: Label Advertisement Mode         IF-Name: Interface name
```

Display detailed information about all LDP-enabled interfaces.

```
<Sysname> display mpls ldp interface verbose
     LDP Interface Information in Public Network
------------------------------------------------------------------------------
 Interface Name : Vlan-interface2
 LDP ID         : 1.1.1.1:0             Transport Address : 1.1.1.1
 Entity Status  : Inactive              Interface MTU     : 1500
 Configured Hello Timer     : 15 Sec
 Negotiated Hello Timer     : 15 Sec
 Configured Keepalive Timer : 45 Sec
 Label Advertisement Mode   : Downstream Unsolicited
 Hello Message Sent/Rcvd    : 0/0 (Message Count)
------------------------------------------------------------------------------
```

display mpls ldp lsp

Syntax

display mpls ldp lsp [**all** | [**vpn-instance** *vpn-instance-name*] [*destination-address mask-length*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all LSPs established by LDP.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

dest-addr: Destination address of the LSP.

mask-length: Length of the mask for the destination address, in the range 0 to 32.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp lsp** command to display information about LSPs established by LDP.

Related commands: **display mpls ldp**.

Examples

Display information about all LSPs established by LDP.

```
<Sysname> display mpls ldp lsp
                              LDP LSP Information
--------------------------------------------------------------------------------
 SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
--------------------------------------------------------------------------------
 1      1.1.1.1/32         3/NULL        127.0.0.1        -------/InL0
 2      10.1.1.0/24        3/NULL        10.1.1.1         -------/Eth1/1
*3      100.1.1.1/32       Liberal(1025)
--------------------------------------------------------------------------------A '*' before an
LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

display mpls ldp peer

Syntax

display mpls ldp peer [**all** [**verbose**] | [**vpn-instance** *vpn-instance-name*] [*peer-id* | **verbose**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Display information about all peers.

verbose: Displays detailed information.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

peer-id: LSR ID of the peer.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp peer** command to display information about specified peers or all peers.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Display information about all peers.

```
<Sysname> display mpls ldp peer
         LDP Peer Information in Public network
 Total number of peers: 3
 ------------------------------------------------------------
 Peer-ID               Transport-Address  Discovery-Source
 ------------------------------------------------------------
 172.17.1.2:0          172.17.1.2         Vlan-interface1
 168.1.1.1:0           168.1.1.1          Vlan-interface2
 100.10.1.1:0          100.10.1.1         Vlan-interface3
 ------------------------------------------------------------
```

Display detailed information about all peers.

```
<Sysname> display mpls ldp peer verbose
        LDP Peer Information in Public network
 ------------------------------------------------------------
```

```
 Peer LDP ID         : 172.17.1.2:0
 Peer Max PDU Length : 4096           Peer Transport Address : 172.17.1.2
 Peer Loop Detection : Off            Peer Path Vector Limit : 0
 Peer FT Flag        : Off            Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----           Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Vlan-interface1
-------------------------------------------------------------
 Peer LDP ID         : 168.1.1.1:0
 Peer Max PDU Length : 4096           Peer Transport Address : 168.1.1.1
 Peer Loop Detection : Off            Peer Path Vector Limit : 0
 Peer FT Flag        : Off            Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----           Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Vlan-interface2
-------------------------------------------------------------
 Peer LDP ID         : 100.10.1.1:0
 Peer Max PDU Length : 4096           Peer Transport Address : 100.10.1.1
 Peer Loop Detection : Off            Peer Path Vector Limit : 0
 Peer FT Flag        : Off            Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----           Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Vlan-interface3
 -------------------------------------------------------------
```

display mpls ldp remote-peer

Syntax

display mpls ldp remote-peer [**remote-name** *remote-peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

remote-peer-name: Name of the remote peer, a case-insensitive string of 1 to 32 characters.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp remote-peer** command to display information about remote LDP peers.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view), **remote-ip**.

Examples

Display information about remote peer BJI.

```
<Sysname> display mpls ldp remote-peer remote-name BJI
                        LDP            Remote            Entity            Information
------------------------------------------------------------------------------

 Remote Peer Name  : BJI
 Remote Peer IP    : 3.3.3.3          LDP ID : 1.1.1.1:0
 Transport Address : 1.1.1.1

 Configured Keepalive Timer : 45 Sec
 Configured Hello Timer     : 45 Sec
 Negotiated Hello Timer     : 45 Sec
 Hello Message Sent/Rcvd    : 3/2 (Message Count)
------------------------------------------------------------------------------
```

display mpls ldp session

Syntax

display mpls ldp session [**all** [**verbose**] | [**vpn-instance** *vpn-instance-name*] [*peer-id* | **verbose**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all information.

verbose: Displays detailed information.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters. Specify this argument to display information about all LDP sessions of a specified VPN.

peer-id: LSR ID of the peer.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp session** command to display information about LDP sessions.

If you do not specify any parameter, the command displays information about all public network LDP sessions.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Display information about all public network LDP sessions.

```
<Sysname> display mpls ldp session
               LDP Session(s) in Public Network
 Total number of sessions: 1
------------------------------------------------------------------------------
 Peer-ID            Status        LAM  SsnRole  FT   MD5  KA-Sent/Rcv
------------------------------------------------------------------------------
 1.1.1.1:0          Operational   DU   Active   Off  Off  4582/4582
------------------------------------------------------------------------------
 LAM : Label Advertisement Mode         FT  : Fault Tolerance
```

Table 1-4 display mpls ldp session command output description

Field	Description
SsnRole	Role of the current LSR in the session, Active or Passive
KA-Sent/Rcv	Number of sent Keepalives and that of received Keepalives during the session

Display detailed information about all public network LDP sessions.

```
<Sysname> display mpls ldp session verbose
             LDP Session(s) in Public Network
------------------------------------------------------------------------------
 Peer LDP ID     : 1.1.1.1:0            Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 -> 1.1.1.1
 Session State   : Operational          Session Role   : Active
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---

 Negotiated Keepalive Timer        : 45 Sec
 Keepalive Message Sent/Rcvd       : 6/6 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Peer Discovery Mechanism          : Extended
 Session existed time              : 000:00:01  (DDD:HH:MM)
 LDP Extended Discovery Source     : Remote peer: 1

 Addresses received from peer: (Count: 2)
 10.1.1.1           1.1.1.1
```

```
--------------------------------------------------------------------------
 Peer LDP ID     : 2.2.2.2:0            Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 -> 2.2.2.2
 Session State   : Operational          Session Role   : Active
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---

 Negotiated Keepalive Timer        : 45 Sec
 Keepalive Message Sent/Rcvd       : 25/25 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Peer Discovery Mechanism          : Basic
 Session existed time              : 000:00:06  (DDD:HH:MM)
 LDP Basic Discovery Source        : Ethernet1/1

 Addresses received from peer: (Count: 3)
 10.1.1.2            20.1.1.1            2.2.2.2

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

Table 1-5 display mpls ldp session verbose output description

Field	Description
Session Role	Role of the current LSR in the session, Active or Passive
Session FT Flag	Whether GR FT is enabled on the peer for the session
MD5 Flag	Whether MD5 authentication is enabled on the peer
Reconnect Timer	GR reconnect timer
Recovery Timer	GR recovery timer
Label Resource Status(Peer/Local)	Whether there are free labels locally and on the peer
Peer Discovery Mechanism	Discovery mechanism of the peer: Basic or Extended
Session existed time	Length of time that elapsed since the session is established
LDP Basic Discovery Source	Interface where the session is established. The value is the name of the interface for basic discovery and name of the remote peer for extended discovery.
LDP Extended Discovery Source	
Addresses received from peer	Addresses received from the peer during the session

display mpls ldp vpn-instance

Syntax

display mpls ldp vpn-instance *vpn-instance-name* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls ldp vpn-instance** command to display information about a specified LDP instance.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Display information about the LDP instance corresponding to VPN instance **vpn1**.

```
<Sysname> display mpls ldp vpn-instance vpn1
                          LDP Global Information
------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 60 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 60 Sec
 MTU Signaling           : Off           Recovery Timer       : 60 Sec

                         LDP Instance Information
------------------------------------------------------------------------
 Instance ID             : 1            VPN-Instance         : vpn1
 Instance Status         : Active       LSR ID               : 1.1.1.9
 Hop Count Limit         : 32           Path Vector Limit    : 32
 Loop Detection          : Off
 DU Re-advertise Timer   : 30 Sec       DU Re-advertise Flag : On
 DU Explicit Request     : Off          Request Retry Flag   : On
 Label Distribution Mode : Ordered      Label Retention Mode : Liberal
```

Note

For description on the fields of the command output, see Table 1-3.

---

display mpls lsp

Syntax

display mpls lsp [**incoming-interface** *interface-type interface-number*] [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**asbr** | [**vpn-instance** *vpn-instance-name*] [**protocol** { **bgp** | **bgp-ipv6** | **ldp** | **static** }]] [**egress** | **ingress** | **transit**] [{ **exclude** | **include** } *dest-addr mask-length*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

incoming-interface *interface-type interface-number*: Specifies LSPs using the given interface as the incoming interface. The *interface-type interface-number* combination specifies an interface by its type and number.

outgoing-interface *interface-type interface-number*: Specifies LSPs using the given interface as the outgoing interface. The *interface-type interface-number* combination specifies an interface by its type and number.

in-label *in-label-value*: Specifies LSPs using the given incoming label. The value of the label ranges 0 to 1048575.

out-label *out-label-value*: Specifies LSPs using the given outgoing label. The value of the label ranges 0 to 1048575.

asbr: Specifies LSPs established by ASBRs.

vpn-instance *vpn-instance-name*: Specifies LSPs of a VPN instance. The VPN instance name is a case-sensitive string of 1 to 31 characters.

protocol: Specifies LSPs established by a given protocol.

bgp: Specifies BGP LSPs.

bgp-ipv6: Specifies IPv6 BGP LSPs, that is, BGP4+ LSPs.

ldp: Specifies LDP LSPs.

static: Specifies static LSPs.

egress: Specifies LSPs taking the current LSR as the egress.

ingress: Specifies LSPs taking the current LSR as the ingress.

transit: Specifies LSPs taking the current LSR as a transit LSR.

exclude: Specifies LSPs other than the one for the given FEC.

include: Specifies the LSP for the given FEC.

dest-addr mask-length: Specifies a FEC by its destination address and the length of the mask. The mask length is in the range 0 to 32.

verbose: Displays detailed information.

Description

Use the **display mpls lsp** command to display information about LSPs.

With no parameters specified, the command displays information about all LSPs.

Related commands: **display mpls lsp**, **display mpls statistics lsp**, **display mpls static-lsp**.

Note

This command supports only VLAN interface.

Examples

Display information about all LSPs.

```
<Sysname> display mpls lsp
--------------------------------------------------------------------------
                 LSP Information: L3VPN LSP
--------------------------------------------------------------------------
FEC              In/Out Label  In/Out IF Route-Distinguisher   Vrf Name
100.1.1.1/32      1025/1024     -/-       100:1                 ASBRLSP

--------------------------------------------------------------------------
                 LSP Information: LDP LSP
--------------------------------------------------------------------------
FEC              In/Out Label  In/Out IF                      Vrf Name
100.10.1.0/24    3/NULL        -/-
100.10.1.0/24    3/NULL        -/-
168.1.0.0/16     3/NULL        -/-
172.17.0.0/16    3/NULL        -/-
```

Table 1-6 display mpls lsp command output description

Field	Description
FEC	Forwarding equivalence class, in either of the following two forms: • IP address/mask: Assigning labels based on destination addresses. • IP address: Assigning labels based on the addresses of the next hops.

Display detailed information about all LSPs.

```
<Sysname> display mpls lsp verbose
------------------------------------------------------------
                 LSP Information: LDP LSP
------------------------------------------------------------
  No.                 :  1
  VrfIndex            :
  Fec                 :  1.1.1.9/32
  Nexthop             :  127.0.0.1
  In-Label            :  3
```

```
Out-Label           :  NULL
In-Interface        :  Vlan-interface3
Out-Interface       :  ----------
LspIndex            :  10241
Tunnel ID           :  0x0
LsrType             :  Egress
Outgoing Tunnel ID  :  0x0
Label Operation     :  POP
```

Table 1-7 display mpls lsp verbose command output description

Field	Description
FEC	Forwarding equivalence class, in either of the following two forms: • IP address/mask: Assigning labels based on destination addresses. • IP address: Assigning labels based on the addresses of the next hops.
Tunnel ID	Tunnel ID (the public network)
LsrType	Role of the LSR for the LSP
Outgoing Tunnel ID	Tunnel ID (inter-AS VPN)

display mpls lsp statistics

Syntax

display mpls lsp statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display mpls lsp statistics** command to display LSP statistics.

Examples

Display LSP statistics.

```
<Sysname> display mpls lsp statistics
Lsp Type       Total     Ingress   Transit   Egress
STATIC LSP     1         1         0         0
STATIC CRLSP   1         1         0         0
LDP LSP        0         0         0         0
CRLDP CRLSP    0         0         0         0
RSVP CRLSP     1         1         0         0
BGP LSP        0         0         0         0
```

```
ASBR LSP       0         0         0         0
BGP IPV6 LSP   0         0         0         0
--------------------------------------------------------------
LSP            1         1         0         0
CRLSP          2         2         0         0
```

Table 1-8 display mpls lsp statistics command output description

Field	Description
Ingress	Number of LSPs taking the current LSR as ingress
Transit	Number of LSPs taking the current LSR as transit LSR
Egress	Number of LSPs taking the current LSR as egress

Note

Currently, the S7900E series switches do not support static CR-LSPs, CR-LDP generated CR-LSPs, or RSVP generated CR-LSPs.

display mpls nhlfe

Syntax

display mpls nhlfe [*token*] [**slot** *slot-number*] [**include** *text*]

View

Any view

Default Level

1: Monitor level

Parameters

token: NHLFE entry index. The value range varies by device.

include *text*: Specifies NHLFE entries including a specified string.

slot *slot-number*: Specifies the NHLFE entries of the board in a slot.

Description

Use the **display mpls nhlfe** command to display information about NHLFE entries.

With the *token* argument not specified, the command displays information about all NHLFE entries.

Examples

Display information about a specified NHLFE entry.

```
<Sysname> display mpls nhlfe 2
Out-Interface       Token      Oper     Nexthop         Deep Stack
------------------------------------------------------------------------
Vlan2                 2        PUSH     88.1.1.2        1    1024
```

Display information about all NHLFE entries.

```
<Sysname> display mpls nhlfe
Out-Interface       Token      Oper     Nexthop         Deep Stack
------------------------------------------------------------------------
Vlan2                 2         PUSH     88.1.1.2        1    1024
```

Table 1-9 display mpls nhlfe command output description

Field	Description
Token	NHLFE entry index
Oper	Operation type
Deep	Depth of the MPLS label stack
Stack	MPLS label

display mpls route-state

Syntax

display mpls route-state [**vpn-instance** *vpn-instance-name*] [*dest-addr mask-length*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies routes of a VPN instance. The VPN instance name is a case-sensitive string of 1 to 31 characters.

dest-addr mask-length: Specifies routes to a destination address. The mask length is in the range 0 to 32.

Description

Use the **display mpls route-state** command to display LSP-related route information.

With no VPN instance specified, the command displays information about the routes of the public network instance.

Examples

Display LSP-related information about all routes.

```
<Sysname> display mpls route-state
DEST/MASK    NEXT-HOP     OUT-INTERFACE   STATE LSP-COUNT  VPN-INDEX
------------------------------------------------------------------
1.1.1.1/32   10.0.0.1     Vlan2           ESTA  1          0
```

Table 1-10 display mpls route-state command output description

Field	Description
LSP-COUNT	Number of LSPs
VPN-INDEX	Index number of the VPN instance

display mpls static-lsp

Syntax

display mpls static-lsp [**lsp-name** *lsp-name*] [{ **exclude** | **include** } *dest-addr mask-length*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

lsp-name *lsp-name*: Specifies an LSP by its name, which is a string of 1 to 15 characters.

exclude: Specifies LSPs other than the one for the given FEC.

include: Specifies the LSP for the given FEC.

dest-addr mask-length: Specifies a FEC by its destination address and the length of the mask. The mask length is in the range 0 to 32.

verbose: Displays detailed information.

Description

Use the **display mpls static-lsp** command to display information about static LSPs.

Related commands: **display mpls lsp**, **display mpls statistics lsp**.

Examples

Display brief information about all static LSPs.

```
<Sysname> display mpls static-lsp
Name       FEC               I/O Label  I/O If                State
lsp1       3.3.3.9/32        NULL/100   -/Vlan1               Up
```

Display detailed information about all static LSPs.

```
<Sysname> display mpls static-lsp verbose
No             : 1
LSP-Name       : lsp1
LSR-Type       : Ingress
FEC            : 3.3.3.9/32
In-Label       : NULL
Out-Label      : 100
In-Interface   : -
```

```
Out-Interface  : Vlan-interface1
NextHop        : 30.1.1.2
Static-Lsp Type: IPTN
Lsp Status     : Up
```

Table 1-11 display mpls static-lsp verbose command output description

Field	Description
LSR-Type	Role of the LSR for the LSP, which can be ingress, egress, or transit
Static-Lsp Type	Type of the static LSP

display mpls statistics interface

Syntax

display mpls statistics interface { *interface-type interface-number* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

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

all: Specifies all interfaces.

Description

Use the **display mpls statistics interface** command to display MPLS statistics for one or all interfaces.

Note that:

To display statistics on a device, set the statistics interval first. By default, the interval is 0 and the system does not collect MPLS statistics. In this case, the value of every statistic is 0.

Related commands: **statistics interval**, **mpls statistics enable**.

Examples

Display MPLS statistics for all interfaces.

```
<Sysname> display mpls statistics interface all
  Statistics for Interface IN :
  Incoming Interface Vlan-interface1
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
       Failed Label Lookup     : 0
       Start Time              : 2008/04/28  10:23:55
       End Time                : 2008/04/28  10:23:55
  Statistics for Interface OUT :
```

```
Outgoing Interface Vlan-interface2
     Octets                 : 0
     Packets                : 0
     Errors                 : 0
     Disables               : 0
     Start Time             : 2008/04/28  10:23:55
     End Time               : 2008/04/28  10:23:55
Statistics for Interface IN :
Incoming Interface Vlan-interface3
     Octets                 : 0
     Packets                : 0
     Errors                 : 0
     Disables               : 0
     Failed Label Lookup    : 0
     Start Time             : 2008/04/28  10:24:04
     End Time               : 2008/04/28  10:24:04
Statistics for Interface OUT :
Outgoing Interface Vlan-interface4
     Octets                 : 0
     Packets                : 0
     Errors                 : 0
     Disables               : 0
     Start Time             : 2008/04/28  10:24:04
     End Time               : 2008/04/28  10:24:04
Statistics for Interface IN :
Incoming Interface Vlan-interface53
     Octets                 : 0
     Packets                : 0
     Errors                 : 0
     Disables               : 0
     Failed Label Lookup    : 0
     Start Time             : 2008/04/28  10:24:10
     End Time               : 2008/04/28  10:24:10
Statistics for Interface OUT :
Outgoing Interface Vlan-interface73
     Octets                 : 0
     Packets                : 0
     Errors                 : 0
     Disables               : 0
     Start Time             : 2008/04/28  10:24:10
     End Time               : 2008/04/28  10:24:10
```

Table 1-12 display mpls statistics interface command output description

Field	Description
Statistics for Interface IN	Statistics for an interface in the incoming direction
Statistics for Interface OUT	Statistics for an interface in the outgoing direction
Octets	Number of bytes processed

Field	Description
Packets	Number of packets processed
Errors	Number of errors
Disables	Number of MPLS disables
Start Time	Start time of the statistics
End Time	End time of the statistics

display mpls statistics lsp

Syntax

display mpls statistics lsp { *index* | **all** | **name** *lsp-name* }

View

Any view

Default Level

1: Monitor level

Parameters

index: Index number of the LSP, in the range 0 to 4294967295.

all: Specifies all LSPs.

lsp-name: Name of the LSP, a string of 1 to 15 characters.

Description

Use the **display mpls statistics lsp** command to display MPLS statistics for all LSPs or the LSP with a specified index or name.

To display MPLS statistics, set the statistics interval first. By default, the interval is 0 and the system does not collect LSP statistics. In this case, the value of every statistic is 0.

Related commands: **statistics interval**.

Examples

Display MPLS statistics for all LSPs.

```
<Sysname> display mpls statistics lsp all
Statistics for Lsp IN : LSP Name /LSP Index :  DynamicLsp/9217
   InSegment
       Octets               : 0
       Packets              : 0
       Errors               : 0
       Down                 : 0
       Start Time           : 2006/05/20  15:52:30
       End Time             : 2006/05/20  15:52:30
  Statistics for Lsp OUT : LSP Name /LSP Index :  DynamicLsp/9217
   OutSegment
```

```
      Octets               : 0
      Packets              : 0
      Errors               : 0
      Down                 : 0
      Start Time           : 0000/00/00  00:00:00
      End Time             : 0000/00/00  00:00:00
 Statistics for Lsp IN : LSP Name /LSP Index :  DynamicLsp/9218
  InSegment
      Octets               : 0
      Packets              : 0
      Errors               : 0
      Down                 : 0
      Start Time           : 0000/00/00  00:00:00
      End Time             : 0000/00/00  00:00:00
 Statistics for Lsp OUT : LSP Name /LSP Index :  DynamicLsp/9218
  OutSegment
      Octets               : 0
      Packets              : 0
      Errors               : 0
      Down                 : 0
      Start Time           : 2006/05/20  15:52:30
      End Time             : 2006/05/20  15:52:30
```

Table 1-13 display mpls statistics lsp command output description

Field	Description
Statistics for Lsp IN : LSP Name /LSP Index : DynamicLsp/10241	Statistics for LSP DynamicLsp/10241 in the incoming direction
InSegment	Information about the LSP in the incoming direction
OutSegment	Information about the LSP in the outgoing direction
Octets	Bytes of data processed
Packets	Number of packets processed
Errors	Number of errors
Down	Number of packets discarded
Start Time	Start time of the statistics
End Time	End time of the statistics

Note

- For an ingress, no statistics is collected in the incoming direction and the start time and end time in the InSegment part of the command output are both 0.
- Similarly, for an egress, no statistics is collected in the outgoing direction and the start time and end time in the OutSegment part of the command output are both 0.

du-readvertise

Syntax

du-readvertise

undo du-readvertise

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

None

Description

Use the **du-readvertise** command to enable label readvertisement for DU mode.

Use the **undo du-readvertise** command to disable the feature.

By default, label readvertisement is enabled in DU mode.

Examples

Enable DU mode label readvertisement for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] du-readvertise
```

Enable DU mode label readvertisement for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] du-readvertise
```

du-readvertise timer

Syntax

du-readvertise timer *value*

undo du-readvertise timer

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

value: Label readvertisement interval, in the range 1 to 65535 seconds.

Description

Use the **du-readvertise timer** command to set the interval for label readvertisement in DU mode.

Use the **undo du-readvertise timer** command to restore the default.

By default, the interval for label readvertisement in DU mode is 30 seconds.

Examples

Set the DU mode label readvertisement interval to 100 seconds for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] du-readvertise timer 100
```

Set the DU mode label readvertisement interval to 100 seconds for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] du-readvertise timer 100
```

graceful-restart (MPLS LDP view)

Syntax

graceful-restart

undo graceful-restart

View

MPLS LDP view

Default Level

1: Monitor level

Parameters

None

Description

Use the **graceful-restart** command to enable MPLS LDP Graceful Restart (GR).

Use the **undo graceful-restart** command to disable MPLS LDP GR.

By default, MPLS LDP GR is disabled.

Note that enabling or disabling GR will cause all LDP sessions and all LSPs based on the sessions to be removed and then reestablished.

Examples

Enable MPLS LDP GR.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart
```

graceful-restart mpls ldp

Syntax

graceful-restart mpls ldp

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **graceful-restart mpls ldp** command to restart MPLS LDP gracefully.

Note that:

- This command is used to test MPLS LDP GR without main/backup switchover. It is not recommended in normal cases.
- The MPLS LDP GR capability is required for this command to take effect.

Related commands: **graceful-restart** (MPLS LDP view).

Examples

Restart MPLS LDP gracefully.

```
<Sysname> graceful-restart mpls ldp
```

graceful-restart timer neighbor-liveness

Syntax

graceful-restart timer neighbor-liveness *timer*

undo graceful-restart timer neighbor-liveness

View

MPLS LDP view

Default Level

1: Monitor level

Parameters

timer: LDP neighbor liveness time, in the range 60 to 300 seconds.

Description

Use the **graceful-restart timer neighbor-liveness** command to set the LDP neighbor liveness time.

Use the **undo graceful-restart timer neighbor-liveness** command to restore the default.

By default, the LDP neighbor liveness time is 120 seconds.

Note that:

- Modifying the LDP neighbor liveness time will cause all LDP sessions and all LSPs based on the sessions to be removed and then reestablished.
- For LDP sessions with MD5 authentication configured, you need to give the LDP neighbor liveness time a greater value so that the TCP connection can be reestablished.

Examples

Set the LDP neighbor liveness time to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer neighbor-liveness 100
```

graceful-restart timer reconnect

Syntax

graceful-restart timer reconnect *timer*

undo graceful-restart timer reconnect

View

MPLS LDP view

Default Level

1: Monitor level

Parameters

timer: Fault Tolerance (FT) reconnect time, in the range 60 to 300 seconds.

Description

Use the **graceful-restart timer reconnect** command to set the FT reconnect time.

Use the **undo graceful-restart timer reconnect** command to restore the default.

By default, the FT reconnect time is 300 seconds.

Note that:

- The FT reconnect time refers to the maximum time that the stale state flag will be preserved by the LSR after the TCP connection fails.
- Modifying the FT reconnect time will cause all LDP sessions and all LSPs based on the sessions to be removed and then reestablished.

Examples

Set the FT reconnect time to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer reconnect 100
```

graceful-restart timer recovery

Syntax

graceful-restart timer recovery *timer*

undo graceful-restart timer recovery

View

MPLS LDP view

Default Level

1: Monitor level

Parameters

timer: LDP recovery time, in the range 3 to 300 seconds.

Description

Use the **graceful-restart timer recovery** command to set the LDP recovery time.

Use the **undo graceful-restart timer recovery** command to restore the default.

By default, the LDP recovery time is 300 seconds.

Note that:

- The LDP recovery time refers to the maximum time that the stale state label will be kept by the LSR after a TCP reconnection.
- Modifying the LDP recovery time will cause all LDP sessions and all LSPs based on the sessions to be removed and then reestablished.

Examples

Set the LDP recovery time to 45 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer recovery 45
```

hops-count

Syntax

hops-count *hop-number*

undo hops-count

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

hop-number: Hop count, in the range 1 to 32.

Description

Use the **hops-count** command to set the maximum hop count for loop detection.

Use the **undo hops-count** command to restore the default.

By default, the maximum hop count for loop detection is 32.

Note that:

- You need to configure this command before enabling LDP on any interface.
- The maximum hop count dictates how fast LDP detects a loop. Adjust this argument as required.

Related commands: **loop-detect**, **path-vectors**.

Examples

Set the maximum hop count for loop detection to 25 for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] hops-count 25
```

Set the maximum hop count for loop detection to 25 for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] hops-count 25
```

label advertise

Syntax

label advertise { **explicit-null** | **implicit-null** | **non-null** }

undo label advertise

View

MPLS view

Default Level

2: System level

Parameters

explicit-null: Specifies that the egress supports PHP and distributes to the penultimate hop an explicit null label, whose value is 0.

implicit-null: Specifies that the egress supports PHP and distributes to the penultimate hop an implicit null label, whose value is 3.

non-null: Specifies that the egress does not support PHP and distributes to the penultimate hop a normal label, whose value is not less than 1024.

Description

Use the **label advertise** command to specify whether the egress should support PHP and what type of label the egress should distribute to the penultimate hop.

Use the **undo label advertise** command to restore the default.

By default, an egress supports PHP and distributes to the penultimate hop an implicit null label.

 **Note**

- The type of label for an egress to distribute depends on whether the penultimate hop supports PHP.
- If LDP sessions have been established, you need to use the **reset mpls ldp** command to reset the sessions to bring the **label advertise** command into effect.

Examples

Configure the egress to distribute an explicit null label to the penultimate hop.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] label advertise explicit-null
```

label-distribution

Syntax

label-distribution { **independent** | **ordered** }

undo label-distribution

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

independent: Works in independent mode, advertising label bindings anytime.

ordered: Works in ordered mode, advertising to its upstream a label binding for a FEC only when it receives a specific label binding message from the next hop of the FEC or it is the egress of the FEC.

Description

Use the **label-distribution** command to specify the label distribution control mode.

Use the **undo label-distribution** command to restore the default.

The default mode is ordered.

Note

If LDP sessions have been established, you must use the **reset mpls ldp** command to reset LDP sessions for this command to take effect.

Examples

Set the label distribution control mode to independent for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] label-distribution independent
```

Set the label distribution control mode to independent for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] label-distribution independent
```

loop-detect

Syntax

loop-detect

undo loop-detect

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

None

Description

Use the **loop-detect** command to enable loop detection.

Use the **undo loop-detect** command to disable loop detection.

By default, loop detection is disabled.

Note that you need to enable loop detection before enabling LDP on any interface.

Related commands: **hops-count**, **path-vectors**.

Examples

Enable loop detection for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] loop-detect
```

Enable loop detection for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] loop-detect
```

lsp-trigger

Syntax

lsp-trigger { **all** | **ip-prefix** *prefix-name* }

undo lsp-trigger { **all** | **ip-prefix** *prefix-name* }

View

MPLS view

Default Level

2: System level

Parameters

all: Specifies all FECs, that is, all static routes and IGP routes.

prefix-name: Name of the IP address prefix list, a string of 1 to 19 characters.

Description

Use the **lsp-trigger** command to configure the LSP establishment triggering policy.

Use the **undo lsp-trigger** command to restore the default.

By default, only loopback addresses with 32-bit masks can trigger LDP to establish LSPs.

Note that:

- With the **all** keyword specified in the **lsp-trigger** command, all static and IGP routes can trigger LDP to establish LSPs.
- With the **ip-prefix** *prefix-name* keyword and argument combination specified in the **lsp-trigger** command, only static and IGP routes permitted by the IP address prefix list can trigger LDP to establish LSPs.
- An IP address prefix list affects only static routes and IGP routes.
- For an LSP to be established, an exactly matching routing entry must exist on the LSR. With loopback addresses using 32-bit masks, only exactly matching host routing entries can trigger LDP to establish LSPs.
- For information about IP address prefix list, refer to *Routing Policy Configuration* in the *IP Routing Volume*.

Examples

Configure LDP to allow all static and IGP routes to trigger LSP establishment.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] lsp-trigger all
```

lsr-id

Syntax

lsr-id *lsr-id*

undo lsr-id

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

lsr-id: LDP LSR ID.

Description

Use the **lsr-id** command to configure an LDP LSR ID.

Use the **undo lsr-id** command to remove a configured LDP LSR ID and all LDP sessions.

By default, the LDP LSR ID takes the value of the MPLS LSR ID.

Examples

Configure the LDP LSR ID of the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] lsr-id 2.2.2.3
```

Configure the LDP LSR ID of LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] lsr-id 4.2.2.3
```

md5-password

Syntax

md5-password { **cipher** | **plain** } *peer-lsr-id password*

undo md5-password *peer-lsr-id*

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

cipher: Displays the password in cipher text.

plain: Displays the password in plain text.

peer-lsr-id: MPLS LSR ID of the peer. An LSR and its peer must use the same password.

password: Password string, case sensitive. If you specify the **plain** keyword, it must be a string of 1 to 16 characters in plain text. If you specify the **cipher** keyword, it can be either a string of 1 to 16 characters in plain text or a string of 24 characters in cipher text.

Description

Use the **md5-password** command to enable LDP MD5 authentication and set the password, which must be the same as that configured on the peer.

Use the **undo md5-password** command to disable LDP MD5 authentication.

By default, LDP MD5 authentication is disabled.

Changing the password will cause the sessions and all LSPs based on the sessions to be removed.

This command takes effect only after MPLS LDP is enabled in the corresponding view.

Examples

Enable MD5 authentication for the public network LDP instance, setting the password display mode to plain text.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] md5-password plain 3.3.3.3 beijingpass
```

Enable MD5 authentication for LDP instance **vpn1**, setting the password display mode to plain text.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] md5-password plain 3.3.3.3 beijingpass
```

mpls

Syntax

mpls

undo mpls

View

System view, interface view

Default Level

2: System level

Parameters

None

Description

Use the **mpls** command in system view to enable MPLS globally and enter MPLS view.

Use the **undo mpls** command in system view to disable MPLS globally.

Use the **mpls** command in interface view to enable MPLS for the interface.

Use the **undo mpls** command in interface view to disable MPLS for the interface.

By default, MPLS capability is not enabled.

Note that:

- You need to configure the LSR ID before enabling MPLS capability.
- You need to enable MPLS globally before enabling it for an interface.

Related commands: **mpls lsr-id**.

Examples

Enable MPLS globally.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
```

Enable MPLS for interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mpls
```

mpls ldp (system view)

Syntax

mpls ldp [**vpn-instance** *vpn-instance-name*]

undo mpls ldp [**vpn-instance** *vpn-instance-name*]

View

System view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

Description

Use the **mpls ldp** command to enable LDP globally and enter MPLS LDP view.

Use the **undo mpls ldp** command to disable LDP globally and remove all LDP instances.

Use the **mpls ldp vpn-instance** command to enable LDP for a VPN instance, create an LDP instance, and enter MPLS LDP VPN instance view.

Use the **undo mpls ldp vpn-instance** command to disable LDP for a VPN instance and remove the LDP instance.

By default, MPLS LDP is disabled.

Configure the **mpls ldp** command after configuring the MPLS LSR ID and enabling MPLS globally.

Examples

Enable LDP globally and enter MPLS LDP view.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
[Sysname] mpls ldp
[Sysname-mpls-ldp]
```

Enable LDP for VPN instance vpn1 and enter MPLS LDP VPN instance view.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1]
```

mpls ldp (interface view)

Syntax

mpls ldp

undo mpls ldp

View

Interface view

Default Level

1: Monitor level

Parameters

None

Description

Use the **mpls ldp** command to enable LDP on an interface.

Use the **undo mpls ldp** command to disable LDP on an interface.

By default, LDP is disabled on an interface.

After you enable LDP on an interface, the interface will periodically send Hello messages.

Before enabling LDP in interface view, be sure to complete the following tasks:

- Use the **mpls lsr-id** command in system view to configure the LSR ID.
- Use the **mpls** command in system view to enable MPLS.
- Use the **mpls ldp** command in system view to enable MPLS LDP globally.
- Use the **mpls** command in interface view to enable MPLS for the interface.

If the interface is bound to a VPN instance, you need to use the **mpls ldp vpn-instance** command to enable LDP for the VPN instance before enabling LDP on the interface.

 **Note**

Currently, this command supports only VLAN interface.

Examples

Enable LDP for interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mpls
[Sysname-Vlan-interface1] mpls ldp
```

mpls ldp remote-peer

Syntax

mpls ldp remote-peer *remote-peer-name*

undo mpls ldp remote-peer *remote-peer-name*

View

System view

Default Level

1: Monitor level

Parameters

remote-peer-name: Name of the remote peer, a case-insensitive string of 1 to 32 characters.

Description

Use the **mpls ldp remote-peer** command to create a remote peer entity and enter MPLS LDP remote peer view.

Use the **undo mpls ldp remote-peer** command to remove a remote peer entity.

Related commands: **remote-ip**.

Examples

Create a remote peer entity named **BJI** and enter MPLS LDP remote peer view.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji]
```

mpls ldp timer hello-hold

Syntax

mpls ldp timer hello-hold *value*

undo mpls ldp timer hello-hold

View

Interface view, MPLS LDP remote peer view

Default Level

1: Monitor level

Parameters

value: Length of time for the Hello timer, in the range 1 to 65535 seconds.

Description

Use the **mpls ldp timer hello-hold** command to set a Hello timer.

Use the **undo mpls ldp timer hello-hold** command to restore the default.

In interface view, you can set the link Hello timer; in MPLS LDP remote peer view, you can set the targeted Hello timer.

By default, the value of the link Hello timer is 15 seconds, and that of the targeted Hello timer is 45 seconds.

 **Note**

Changing the values of the Hello timers does not affect any existing session.

Related commands: **mpls ldp** (system view), **mpls ldp** (interface view).

Examples

Set the link Hello timer to 100 seconds on interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mpls
[Sysname-Vlan-interface1] mpls ldp
[Sysname-Vlan-interface1] mpls ldp timer hello-hold 100
```

Set the targeted Hello timer to 1000 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp timer hello-hold 1000
```

mpls ldp timer keepalive-hold

Syntax

mpls ldp timer keepalive-hold *value*

undo mpls ldp timer keepalive-hold

View

Interface view, MPLS LDP remote peer view

Default Level

1: Monitor level

Parameters

value: Length of time for the Keepalive timer, in the range 1 to 65535 seconds.

Description

Use the **mpls ldp timer keepalive-hold** command to set a keepalive timer.

Use the **undo mpls ldp timer keepalive-hold** command to restore the default.

In interface view, you can set the link Keepalive timer; in MPLS LDP remote peer view, you can set the targeted Keepalive timer.

By default, both the link Keepalive timer and targeted Keepalive timer are set to 45 seconds.

Caution

- If more than one link with LDP enabled exists between two LSRs (for example, when the two LSRs are connected through multiple interfaces), the Keepalive timers of all the links must be identical for the sessions to be stable.
- Changing the values of the Keepalive timers will cause all LDP sessions and the LSPs based on the sessions to be removed and then reestablished.

Examples

Set the link Keepalive timer to 50 seconds on interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mpls
[Sysname-Vlan-interface1] mpls ldp
[Sysname-Vlan-interface1] mpls ldp timer keepalive-hold 50
```

Set the targeted Keepalive timer to 1000 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp timer keepalive-hold 1000
```

mpls ldp transport-address

Syntax

mpls ldp transport-address { *ip-address* **| interface** }

undo mpls ldp transport-address

View

Interface view, MPLS LDP remote peer view

Default Level

1: Monitor level

Parameters

ip-address: IP address for LDP to use as the TCP transport address.

interface: Specifies that LDP use the IP address of the current interface as the TCP transport address. This keyword is available only in interface view.

Description

Use the **mpls ldp transport-address** command to configure an LDP transport address.

Use the **undo mpls ldp transport-address** command to restore the default.

By default, a transport address takes the value of the MPLS LSR ID.

In interface view, you configure the link Hello transport address; in MPLS LDP remote peer view, you configure the targeted Hello transport address.

Examples

On interface VLAN-interface 1, configure the link Hello transport address as the IP address of the current interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mpls
[Sysname-Vlan-interface1] mpls ldp
[Sysname-Vlan-interface1] mpls ldp transport-address interface
```

Configure the targeted Hello transport address to be 10.1.1.1.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp transport-address 10.1.1.1
```

mpls lsr-id

Syntax

mpls lsr-id *lsr-id*

undo mpls lsr-id

View

System view

Default Level

2: System level

Parameters

lsr-id: ID for identifying the LSR, in dotted decimal notation.

Description

Use the **mpls lsr-id** command to configure the ID of an LSR.

Use the **undo mpls lsr-id** command to remove the ID of an LSR.

By default, no LSR ID is configured.

Your need to configure the LSR ID of an LSR before configuring any other MPLS commands.

You are recommended to use the address of a loopback interface on the LSR as the ID.

Related commands: **display mpls interface**.

Examples

Set the LSR ID to 3.3.3.3.

```
<Sysname> system-view
[Sysname] mpls lsr-id 3.3.3.3
```

path-vectors

Syntax

path-vectors *pv-number*

undo path-vectors

View

MPLS LDP view, MPLS LDP VPN instance view

Default Level

1: Monitor level

Parameters

pv-number: Maximum path vector length, in the range 1 to 32.

Description

Use the **path-vectors** command to set the maximum path vector length.

Use the **undo path-vectors** command to restore the default.

By default, the maximum path vector length for an instance is 32.

Note that this command must be configured before you enable MPLS LDP on any interface.

Related commands: **loop-detect**, **hops-count**.

Examples

Set the maximum path vector length to 3 for the public network LDP instance.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] path-vectors 3
```

Set the maximum path vector length to 3 for LDP instance **vpn1**.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] path-vectors 3
```

ping lsp

Syntax

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ipv4** *dest-addr mask-length* [*destination-ip-addr-header*]

View

Any view

Default Level

0: Visit level

Parameters

-a *source-ip*: Specifies the source address for the echo request messages.

-c *count*: Specifies the number of request messages to be sent. The *count* argument ranges from 1 to 4294967295.

-exp *exp-value*: Specifies the EXP value for the echo request message. The *exp-value* argument ranges from 0 to 7.

-h *ttl-value*: Specifies the TTL value for the echo request message. The *ttl-value* argument ranges from 1 to 255.

-m *wait-time*: Specifies the interval for sending echo request messages. The *wait-time* argument ranges from 1 to 10,000 ms.

-r *reply-mode*: Specifies the reply mode in response to an echo request message. The *reply-mode* argument can be 1 or 2. A value of 1 means “Do not response”, while a value of 2 means “Respond using a UDP packet”.

-s *packet-size*: Specifies the payload length of the echo request message. The *packet-size* argument ranges from 64 to 8100 bytes.

-t *time-out*: Specifies the timeout interval for the response to an echo request message. The *time-out* argument ranges from 0 to 65535 milliseconds.

-v: Displays detailed response information.

ipv4 *dest-addr mask-length*: Specifies the IPv4 destination address of the LSP and the mask. The *mask-length* argument ranges from 0 to 32.

destination-ip-addr-header: Specifies the IP header destination address for the MPLS echo request messages. It can be any address on segment 127.0.0.0/8, that is, any local loopback address.

Description

Use the **ping lsp** command to check the validity and reachability of an LSP.

Examples

Ping a specified address, sending five packets.

```
<Sysname> ping lsp –c 5 ipv4 3.3.3.9 32
LSP PING FEC: LDP IPV4 PREFIX 3.3.3.9/32 : 100  data bytes, press CTRL_C to break
    Reply from 100.1.2.1: bytes=100 Sequence=0 time = 31 ms
    Reply from 100.1.2.1: bytes=100 Sequence=1 time = 62 ms
    Reply from 100.1.2.1: bytes=100 Sequence=2 time = 62 ms
```

```
  Reply from 100.2.3.1: bytes=100 Sequence=3 time = 62 ms
  Reply from 100.1.2.1: bytes=100 Sequence=4 time = 62 ms

--- FEC: LDP IPV4 PREFIX 3.3.3.9/32 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/55/62 ms
```

remote-ip

Syntax

remote-ip *ip-address*

undo remote-ip

View

MPLS LDP remote peer view

Default Level

1: Monitor level

Parameters

ip-address: Remote peer IP address.

Description

Use the **remote-ip** command to configure the remote peer IP address.

Use the **undo remote-ip** command to remove the configuration.

Note that the remote peer IP address must be the MPLS LSR ID of the remote peer. Two peers use their MPLS LSR IDs as the transport addresses to establish the TCP connection.

Related commands: **mpls ldp remote-peer**.

Examples

Configure the remote peer IP address.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
```

reset mpls ldp

Syntax

reset mpls ldp [**all** | [**vpn-instance** *vpn-instance-name*] [*fec mask* | **peer** *peer-id*]]

View

User view

Default Level

2: System level

Parameters

all: Specifies all LDP instances, including the public one and private ones.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

fec mask: Specifies a FEC by the destination IP address and mask.

peer *peer-id*: Specifies a peer by its LSR ID.

Description

Use the **reset mpls ldp** command to reset LDP sessions.

With no parameters specified, the command resets all sessions of the public network LDP instance.

Examples

Reset all sessions of the public network LDP instance.

```
<Sysname> reset mpls ldp
```

Reset the sessions of all LDP instances.

```
<Sysname> reset mpls ldp all
```

Reset the sessions of LDP instance **vpn1**.

```
<Sysname> reset mpls ldp vpn-instance vpn1
```

Reset the sessions of a specified FEC.

```
<Sysname> reset mpls ldp 2.2.2.2 24
```

Reset the sessions with a specified peer.

```
<Sysname> reset mpls ldp peer 2.2.2.9
```

reset mpls statistics interface

Syntax

reset mpls statistics interface { *interface-type interface-number* | **all** }

View

User view

Default Level

2: System level

Parameters

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

all: Specifies all interfaces.

Description

Use the **reset mpls statistics interface** command to clear MPLS statistics for one or all MPLS interfaces.

Related commands: **display mpls statistics interface**.

Examples

Clear MPLS statistics for interface VLAN-interface 1.

```
<Sysname> reset mpls statistics interface vlan-interface 1
```

reset mpls statistics lsp

Syntax

reset mpls statistics lsp { *index* | **all** | **name** *lsp-name* }

View

User view

Default Level

2: System level

Parameters

index: Index number of the LSP, in the range 0 to 4294967295.

all: Specifies all LSPs.

lsp-name: Name of the LSP, a string of 1 to 15 characters.

Description

Use the **reset mpls statistics lsp** command to clear MPLS statistics for all LSPs or the LSP with a specified index or name.

Related commands: **display mpls statistics lsp**.

Examples

Clear MPLS statistics for LSP **lsp1**.

```
<Sysname> reset mpls statistics lsp lsp1
```

static-lsp egress

Syntax

static-lsp egress *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label*

undo static-lsp egress *lsp-name*

View

System view

Default Level

2: System level

Parameters

lsp-name: Name for the LSP, a string of 1 to 15 characters.

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

in-label: Incoming label value, in the range 16 to 1023.

Description

Use the **static-lsp egress** command to configure a static LSP taking the current LSR as the egress.

Use the **undo static-lsp egress** command to remove a static LSP taking the current LSR as the egress.

Related commands: **static-lsp ingress**, **static-lsp transit**, **display mpls static-lsp**.

Examples

Configure a static LSP named bj-sh, taking the current LSR as the egress.

```
<Sysname> system-view
[Sysname] static-lsp egress bj-sh incoming-interface vlan-interface 2 in-label 233
```

static-lsp ingress

Syntax

static-lsp ingress *lsp-name* **destination** *dest-addr* { *mask* | *mask-length* } **nexthop** *next-hop-addr* **out-label** *out-label*

undo static-lsp ingress *lsp-name*

View

System view

Default Level

2: System level

Parameters

lsp-name: Name for the LSP, a string of 1 to 15 characters.

dest-addr: Destination IP address of the LSP.

mask: Mask of the destination IP address.

mask-length: Length of the mask for the destination address, in the range 0 to 32.

next-hop-addr: Address of the next hop.

out-label: Outgoing label, in the range 16 to 1023.

Description

Use the **static-lsp ingress** command to configure a static LSP taking the current LSR as the ingress.

Use the **undo static-lsp ingress** command to remove a static LSP taking the current LSR as the ingress.

Note that:

- If you specify the next hop when configuring a static LSP, and the address of the next hop is present in the routing table, you also need to specify the next hop when configuring the static IP route.
- If you specify the outgoing interface when configuring a static LSP, you also need to specify the outgoing interface when configuring the static IP route.
- The address of the next hop cannot be any local public network IP address.

Related commands: **static-lsp egress**, **static-lsp transit**, **display mpls static-lsp**.

Examples

Configure a static LSP to destination address 202.25.38.1, taking the current LSR as the ingress.

```
<Sysname> system-view
[Sysname] static-lsp ingress bj-sh destination 202.25.38.1 24 nexthop 202.55.25.33 out-label
237
```

static-lsp transit

Syntax

static-lsp transit *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* **nexthop** *next-hop-addr* **out-label** *out-label*

undo static-lsp transit *lsp-name*

View

System view

Default Level

2: System level

Parameters

lsp-name: Name for the LSP, a string of 1 to 15 characters.

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

in-label: Incoming label, in the range 16 to 1023.

next-hop-addr: Address of the next hop.

out-label: Outgoing label, in the range 16 to 1023.

Description

Use the **static-lsp transit** command to configure a static LSP taking the current LSR as a transit LSR.

Use the **undo static-lsp transit** command to remove a static LSP taking the current LSR as a transit LSR.

Note that:

- If you specify the next hop when configuring a static LSP, and the address of the next hop is present in the routing table, you also need to specify the next hop when configuring the static IP route.
- If you specify the outgoing interface when configuring a static LSP, you also need to specify the outgoing interface when configuring the static IP route.
- The address of the next hop cannot be any local public network IP address.

Related commands: **static-lsp egress**, **static-lsp ingress**.

Examples

Configure a static LSP, taking interface Vlan-interface 2 as the incoming interface and setting the incoming label as 123 and the outgoing label as 253.

```
<Sysname> system-view
[Sysname] static-lsp transit bj-sh incoming-interface Vlan-interface 2 in-label 123 nexthop
202.34.114.7 out-label 253
```

statistics interval

Syntax

statistics interval *interval-time*

undo statistics interval

View

MPLS view

Default Level

2: System level

Parameters

interval-time: Statistics Interval, in the range 30 to 65535 seconds.

Description

Use the **statistics interval** command to set the statistics interval, that is, the interval for collecting statistics.

Use the **undo statistics interval** command to restore the default.

By default, the interval is 0, that is, the system does not collect statistics.

Related commands: **display mpls statistics interface**, **display mpls statistics lsp**.

Examples

Set the statistics interval to 30 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] statistics interval 30
```

tracert lsp

Syntax

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* |**-t** *time-out*] * **ipv4** *dest-addr mask-length* [*destination-ip-addr-header*]

View

Any view

Default Level

0: Visit level

Parameters

-a *source-ip*: Specifies the source address for the echo request messages.

-exp *exp-value*: Specifies the EXP value for the echo request messages. The *exp-value* argument ranges from 0 to 7.

-h *ttl-value*: Specifies the TTL value for the echo request messages. The *ttl-value* argument ranges from 1 to 255.

-r *reply-mode*: Specifies the reply mode in response to an echo request message. The *reply-mode* argument can be 1 or 2. A value of 1 means “Do not response”, while a value of 2 means “Respond using a UDP packet”.

-t *time-out*: Specifies the timeout interval for the response to an echo request message. The *time-out* argument ranges from 0 to 65535 milliseconds.

ipv4 *dest-addr mask*: Specifies the LDP IPv4 destination address and the mask. The *mask* argument ranges from 0 to 32.

destination-ip-addr-header: Specifies the IP header destination address for the MPLS echo request messages. It can be any address on segment 127.0.0.0/8, that is, any local loopback address.

Description

Use the **tracert lsp** command to locate an MPLS LSP error.

Examples

Locate an error along the LSP to 3.3.3.9 on host 1.1.1.1.

```
<Sysname> tracert lsp ipv4 3.3.3.9 32
LSP Trace Route FEC: LDP IPV4 PREFIX 3.3.3.9/32 , press CTRL_C to break.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   10.4.5.1/[1025]
  1      10.4.5.1           1       Transit   100.3.4.1/[1024]
  2      100.1.4.2          63      Transit   100.1.2.1/[3]
  3      100.1.2.1          129     Egress
```

ttl expiration pop

Syntax

ttl expiration pop

undo ttl expiration pop

View

MPLS view

Default Level

2: System level

Parameters

None

Description

Use the **ttl expiration pop** command to specify that ICMP responses travel along the IP route when the TTL of an MPLS packet expires.

Use the **undo ttl expiration pop** command to specify that ICMP responses travel along the LSP when the TTL of an MPLS packet expires.

By default, ICMP responses of an MPLS packet with a one-level label stack travel along the IP route.

Note that configuring the **undo mpls** command will remove the configurations of the **ttl expiration pop** command.

Related commands: **ttl propagate**.

Examples

Specify that ICMP responses travel along the LSP when the TTL of an MPLS packet expires.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] undo ttl expiration pop
```

ttl propagate

Syntax

ttl propagate { **public** | **vpn** }

undo ttl propagate { **public** | **vpn** }

View

MPLS view

Default Level

2: System level

Parameters

public: Specifies public network packets.

vpn: Specifies VPN packets.

Description

Use the **ttl propagate** command to enable MPLS IP TTL propagation for public network packets or VPN packets.

Use the **undo ttl propagate** command to disable the function.

By default, MPLS IP TTL propagation is enabled for only public network packets.

Related commands: **ttl expiration pop**.

Examples

Enable MPLS IP TTL propagation for VPN packets.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] ttl propagate vpn
```

Table of Contents

1 MPLS L2VPN Configuration Commands

MPLS L2VPN Configuration Commands

ccc interface in-label out-label

Syntax

ccc *ccc-connection-name* **interface** *interface-type interface-number* **in-label** *in-label-value* **out-label** *out-label-value* **nexthop** *ip-address* [**control-word** | **no-control-word**]

undo ccc *ccc-connection-name*

View

System view

Default Level

2: System level

Parameters

ccc-connection-name: Name for the CCC connection, a string of 1 to 20 characters. It is used for uniquely identifying a CCC connection on a PE.

interface-type interface-number: Specifies the interface connecting the local CE by its type and number.

in-label-value: Incoming label, in the range 16 to 1023.

out-label-value: Outgoing label, in the range 16 to 1023.

nexthop *ip-address*: Specifies the IP address of the next hop.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Note

At present, the S7900E series Ethernet switches do not support the control word option.

Description

Use the **ccc interface in-label out-label** command to create a remote CCC connection between CEs connected to different PEs.

Use the **undo ccc** command to delete a CCC connection.

This command must be configured on both of the PEs.

A PE uses connection names to identify different CCC connections. A CCC connection can have different names on different PEs.

If a P router is connected with a PE, you must configure a static LSPs between them.

Examples

Create a remote CCC connection from CEA to CEB, setting the incoming interface to that connecting CEA, namely VLAN-interface 10; the next hop to 20.1.1.2; the incoming label to 100; and the outgoing label to 200.

```
<Sysname> system-view
[Sysname] ccc CEA-CEB interface vlan-interface 10 in-label 100 out-label 200 nexthop 20.1.1.2
```

ce

Syntax

ce *ce-name* [**id** *ce-id* [**range** *ce-range*] [**default-offset** *ce-offset*]]

undo ce *ce-name*

View

MPLS L2VPN view, MPLS L2VPN CE view

Default Level

2: System level

Parameters

ce-name: Unique name for a CE in the current VPN of the current PE, a string of 1 to 20 characters that cannot include the character of “-”.

ce-id: ID for the CE in the VPN, the range of valid values varies by device.

ce-range: Maximum number of CEs that the current PE can support. The default is 10. The value range varies by device.

ce-offset: Original CE offset. It can be either 0 or 1. The default is 0.

Description

Use the **ce** command in MPLS L2VPN view to create a CE and enter MPLS L2VPN CE view.

Use the **undo ce** command to delete a CE.

Note

To create a CE, you need to specify the **id** keyword in the command; to enter the view of an existing CE, you do not need to do so.

Examples

Create a CE named ce1 for a VPN.

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

```
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 100:1
[Sysname-mpls-l2vpn-vpn1] ce ce1 id 1
[Sysname-mpls-l2vpn-ce-vpn1-ce1]
```

Create a CE named ce2 for a VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 100:1
[Sysname-mpls-l2vpn-vpn1] ce ce1 id 1
[Sysname-mpls-l2vpn-ce-vpn1-ce1] ce ce1 id 2
[Sysname-mpls-l2vpn-ce-vpn1-ce2]
```

connection

Syntax

connection [**ce-offset** *id*] **interface** *interface-type interface-number* [**tunnel-policy** *tunnel-policy-name*]

undo connection { **ce-offset** *id* | **interface** *interface-type interface-number* }

View

MPLS L2VPN CE view

Default Level

2: System level

Parameters

ce-offset *id*: Specifies the ID of the peer CE of the L2VPN connection, in the range 0 to 199.

interface-type interface-number: Specifies the interface connecting the CE by its type and number. The encapsulation type must be same as that of the VPN.

tunnel-policy *tunnel-policy-name*: Specifies a tunneling policy for the VC, which is a string of 1 to 19 characters.

Description

Use the **connection** command to create a Kompella connection.

Use the **undo connection** command to delete a Kompella connection on a CE interface.

When creating a Kompella connection, you must specify the ID of the peer CE and the local CE interface.

If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number of one.

Related commands: **tunnel select-seq load-balance-number** in *MPLS L3VPN Commands* of the *MPLS Volume*.

Examples

Create a Kompella connection.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1
[Sysname-mpls-l2vpn-vpn1] ce ce1
[Sysname-mpls-l2vpn-ce-vpn1-ce1] connection ce-offset 1 interface vlan-interface 10
```

display bgp l2vpn

Syntax

display bgp l2vpn { **all** | **group** [*group-name*] | **peer** [[*ip-address*] **verbose**] | **route-distinguisher** *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]] }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all L2VPN information.

group-name: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

verbose: Displays detailed information.

route-distinguisher: Route distinguisher in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters.

ce-id: VPN CE ID of the MPLS L2VPN connection, in the range 0 to 199. A remote connection requires the remote CE number.

label-offset: Label offset, in the range 0 to 65,535.

Description

Use the **display bgp l2vpn** command to display information about BGP L2VPN in the BGP routing table.

Related commands: **route-distinguisher.**

Examples

Display all information about L2VPN in the BGP routing table.

```
<Sysname> display bgp l2vpn all
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 bgp.l2vpn: 1 destination
 Route Distinguisher: 100:1
 CE ID   Label Offset   Label Base    nexthop          pref   as-path
 1       0              8202          3.3.3.9          100
```

Table 1-1 display bgp l2vpn all command output description

Field	Description
Origin codes	Route origin codes, which can be: i – IGP: Indicates that the network layer reachability information is from within the AS e – EGP: Indicates that the network layer reachability information is learned through EGP ? – incomplete: Indicates that the network layer reachability information is learned through other ways
bgp.l2vpn	Number of BGP L2VPNs
CE ID	CE number in the VPN
nexthop	IP address of the next hop
pref	Local preference
as-path	AS-PATH of the route

Display brief information about L2VPN peers in the BGP routing table.

```
<Sysname> display bgp l2vpn peer

 BGP local router ID : 4.4.4.9
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 0

  Peer        V   AS   MsgRcvd   MsgSent  OutQ PrefRcv Up/Down  State

  3.3.3.9     4   100        0        0     0       0  00:01:07 Active
```

Table 1-2 display bgp l2vpn peer command output description

Field	Description
BGP local router ID	ID of the local BGP router
Peers in established state	Number of peers with BGP sessions in the state of established
Peer	IP address of the peer
V	BGP version that the peer is using
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration that the BGP session is in the current status
State	Status of the peer

Display detailed information about L2VPN peer 3.3.3.9 in the BGP routing table.

```
<Sysname> display bgp l2vpn peer 3.3.3.9 verbose
```

```
        Peer: 3.3.3.9   Local: 2.2.2.9
        Type: IBGP link
        BGP version 4, remote router ID 3.3.3.9
        BGP current state: Established, Up for   00:21:15
        BGP current event: KATimerExpired
        BGP last state: OpenConfirm
        Port:  Local - 179      Remote - 1034
        Configured: Active Hold Time: 180 sec   Keep Alive Time:60 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 180 sec
        Peer optional capabilities:
        Peer support bgp multi-protocol extended
        Peer support bgp route refresh capability
        Address family IPv4 Unicast: advertised and received
        Address family L2VPN: advertised and received
Received: Total 26 messages, Update messages 2
Sent: Total 28 messages, Update messages 2
Maximum allowed prefix number: 150000
Threshold: 75%
Minimum time between advertisement runs is 15 seconds
Peer Preferred Value: 0
 BFD: Enabled
Routing policy configured:
No routing policy is configured
```

Table 1-3 display bgp l2vpn peer verbose command output description

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP current state	Current status of the BGP session
BGP current event	Current event of the BGP session
BGP last state	Last status of the BGP session
Port	Ports used by the BGP session, one is local or the other remote
Configured	Settings of the local timers
Received	Settings of the remote timers
Negotiated	Negotiated settings of the timers
Peer optional capabilities: Peer support bgp multi-protocol extended Peer support bgp route refresh capability	Optional peer capabilities, including the support for BGP multicast protocol extension and the support for BGP route refreshing
Address family IPv4 Unicast	IPv4 unicast address family capability
Address family L2VPN	L2VPN address family

Field	Description
Received	Total number of received messages and that of received update messages
Sent	Total number of sent messages and that of received update messages
Maximum allowed prefix number	Maximum number of routes allowed
Threshold	Threshold value
BFD	Whether BFD is enabled for the peer
Routing policy configured	Routing policy specified for the peer

Display L2VPN information with the RD being 100:1 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 bgp.l2vpn: 1 destination
 CE ID   Label Offset   Label Base    nexthop        pref    as-path
 4       0              132096        3.3.3.9        100
```

Table 1-4 display bgp l2vpn route-distinguisher command output description

Field	Description
Origin codes	Route origin codes, which can be: i – IGP: Indicates that the network layer reachability information is from within the AS e – EGP: Indicates that the network layer reachability information is learned through EGP ? – incomplete: Indicates that the network layer reachability information is learned through other ways
bgp.l2vpn	Number of BGP L2VPNs
CE ID	CE number in the VPN
nexthop	IP address of the next hop
pref	Preference
as-path	AS-PATH of the route

Display L2VPN information with the RD being 100:1 and the CE ID being 4 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1 ce-id 4
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 CE ID   Label Offset   Label Base    nexthop          pref   as-path
 1       0              8202          3.3.3.9          100
```

Table 1-5 display bgp l2vpn route-distinguisher ce-id command output description

Field	Description
Origin codes	Route origin codes, which can be: i – IGP: Indicates that the network layer reachability information is from within the AS e – EGP: Indicates that the network layer reachability information is learned through EGP ? – incomplete: Indicates that the network layer reachability information is learned through other ways
CE ID	CE number in the VPN
nexthop	IP address of the next hop
pref	Preference
as-path	AS-PATH of the route

Display L2VPN information with the RD being 100:1, the CE ID being 4, and the label offset being 0 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1 ce-id 4 label-offset 0
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 nexthop:3.3.3.9,  pref :100,     as-path :
 label base:132096,label range:10,layer-2 mtu:0,encap type:Unknown or Reserved
  label            state
  132096           down
  132097           up
  132098           down
  132099           down
  132100           down
  132101           down
  132102           down
  132103           down
  132104           down
  132105           down
```

The following table gives the description on the fields of the **display bgp l2vpn route-distinguisher ce-id label-offset** command.

Table 1-6 Output description

Field	Description
Origin codes	Route origin codes, which can be: i – IGP: Indicates that the network layer reachability information is from within the AS e – EGP: Indicates that the network layer reachability information is learned through EGP ? – incomplete: Indicates that the network layer reachability information is learned through other ways
nexthop	IP address of the next hop

Field	Description
pref	Preference
as-path	AS-PATH of the route
encap type	Encapsulation type

display ccc

Syntax

display ccc [**ccc-name** *ccc-name* | **type** { **local** | **remote** }]

View

Any view

Default Level

1: Monitor level

Parameters

ccc-name: CCC connection name, a string of 1 to 20 characters..

type: Specifies the type of the CCC connections.

local: Specifies local CCC connections.

remote: Specifies remote CCC connections.

Description

Use the **display ccc** command to display information about CCC connections.

If you do not specify the connection name or type, this command displays information about all CCC connections.

Examples

Display information about CCC connection c1.

```
<Sysname> display ccc ccc-name c1
     ***Name                    : c1
        Type                    : remote
        State                   : down
        Intf                    : Vlan-interface2 (up)
        In-label                : 100
        Out-label               : 200
        Nexthop                 : 20.1.1.1
```

Display information about all CCC connections.

```
<Sysname> display ccc
    Total  ccc vc          : 1
    Local  ccc vc          : 0,  0 up
    Remote ccc vc          : 1,  0 up
 ***Name                   : c1
    Type                   : remote
```

```
State                : down
Intf                 : Vlan-interface2 (up)
In-label             : 100
Out-label            : 200
Nexthop              : 20.1.1.1
```

Table 1-7 display ccc command output description

Field	Description
Total ccc vc	Total number of CCC connections
Local ccc vc	Number of local CCC connections
Remote ccc vc	Number of remote CCC connections
Name	Name of the CCC connection
Type	Type of the CCC connection
State	Status of the CCC connection
Intf	Interface of the CCC connection
In-label	Incoming label
Out-label	Outgoing label
Nexthop	IP address of the next hop

display l2vpn ccc-interface vc-type

Syntax

display l2vpn ccc-interface vc-type { **all** | **bgp-vc** | **ccc** | **ldp-vc** | **static-vc** } [**up** | **down**]

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies interfaces of any encapsulation types.

bgp-vc: Specifies interfaces of Kompella L2VPN VCs.

ccc: Specifies interfaces of CCC L2VPN VCs.

ldp-vc: Specifies interfaces of Martini L2VPN VCs.

static-vc: Specifies interfaces of SVC L2VPN VCs.

up: Specifies CCC interfaces in the state of UP.

down: Specifies CCC interfaces in the state of DOWN.

Description

Use the **display l2vpn ccc-interface vc-type** command to display information about specified L2VPN VC interfaces.

Examples

Display information about interfaces of any encapsulation types.

```
<Sysname> display l2vpn ccc-interface vc-type all
Total ccc-interface of CCC VC: 3
up (3), down (0)
Interface     Encap Type  State   VC Type
Vlan2         ethernet     up      CCC
Vlan3         ethernet     up      bgp-vc
Vlan4         ethernet     up      static-vc
```

Display information about interfaces of Kompella L2VPN VCs.

```
<Sysname> display l2vpn ccc-interface vc-type bgp-vc
Total ccc-interface of BGP VC: 1
up (1), down (0)
Interface     Encap Type  State   VC Type
Vlan3         ethernet         up      bgp-vc
```

Display information about interfaces of SVC L2VPN VCs that are in the state of UP.

```
<Sysname> display l2vpn ccc-interface vc-type svc-vc up
Total ccc-interface of SVC VC: 1,
up (1), down (0)
Interface     Encap Type  State   VC Type
Vlan4         VLAN         up      static-vc
```

Table 1-8 display l2vpn ccc-interface vc-type command output description

Field	Description
Total ccc-interface of XXX VC	Total interface number of L2VPN VCs of type xxx
Interface	Name of the interface
Encap Type	Encapsulation type of the interface
State	Status of the interface
VC Type	Encapsulation type of the L2VPN VC interface

display mpls l2vc

Syntax

display mpls l2vc [**interface** *interface-type interface-number* | **remote-info**]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies the interface connecting the CE by its type and number.

remote-info: Specifies Martini VCs from the remote peer.

Description

Use the **display mpls l2vc** command to display information about Martini VCs configured on the router.

If you specify an interface, the command displays information about Martini VCs configured on the CE interface.

Examples

Display information about all Martini VCs configured on the router.

```
<Sysname> display mpls l2vc
total  ldp vc : 3     0 up       3 down
Transport  Client       VC      Local      Remote     Tunnel
VC ID      Intf         State   VC Label   VC Label   Policy
5          Vlan2        down    0          0          lsp3
6          Vlan3        down    0          0          lsp2
7          Vlan4        down    0          0          plcy3
```

Table 1-9 display mpls l2vc command output description

Field	Description
total ldp vc	Total number of Martini VCs
Transport VC ID	Remote VC ID
Client Intf	Interface connected with the CE
VC State	Status of the VC
Remote VC Label	Remote VC label
Tunnel Policy	Tunnel policy configured

Display information about Martini VCs received from the remote peer.

```
<Sysname> display mpls l2vc remote-info
total remote ldp vc : 1
Transport  Group      Peer            Remote     Remote     C     Remote
VC ID      ID         Addr            Encap      VC Label   Bit   MTU
100        0          3.3.3.9         ethernet   1025       0     1500
```

Table 1-10 display mpls l2vc remote-info command output description

Field	Description
total remote ldp vc	Total number of remote LDP VCs
Transport VC ID	Remote VC ID
Group ID	Remote VC group ID, used for the L2VPN VC FEC TLV field of LDP messages
Peer Addr	IP address of the peer

Field	Description
Remote Encap	Encapsulation type of the remote interface
C Bit	Control word, which can be 0 or 1
Remote MTU	MTU of the remote interface

display mpls l2vpn

Syntax

display mpls l2vpn [**export-route-target-list** | **import-route-target-list** | **vpn-name** *vpn-name* [**local-ce** | **remote-ce**]]

View

Any view

Default Level

1: Monitor level

Parameters

export-route-target-list: Displays the export route target list.

import-route-target-list: Displays the import route target list.

vpn-name: VPN name, a case insensitive string of 1 to 31 characters that cannot include the character of "-".

local-ce: Displays the configurations and status of all local CEs of a specified VPN.

remote-ce: Displays the configurations and status of remote CEs learned from other PEs.

Description

Use the **display mpls l2vpn** command to display information about L2VPNs configured on a PE.

If you do not specify a VPN, the command displays information about all L2VPNs.

Examples

Display the L2VPN export route target list.

```
<Sysname> display mpls l2vpn export-route-target-list
export vpn target list: 755:7  888:8
```

Table 1-11 display mpls l2vpn export-route-target-list command output description

Field	Description
export vpn target list	BGP VPN export route target list

Display information about all L2VPNs configured on the PE.

```
<Sysname> display mpls l2vpn
VPN Number: 1
 vpn-name  encap-type  route-distinguisher     mtu   ce(L)  ce(R)
 vpn2      ethernet    500:1                   888   0      0
```

Table 1-12 display mpls l2vpn command output description

Field	Description
VPN Number	Number of created VPNs
vpn-name	Name of the VPN
encap-type	Encapsulation type
mtu	Maximum transmission unit
ce(L)	Local CE number
ce(R)	Remote CE number

Display information about L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1
 ***VPN name               : vpn1
    Encap type             : vlan
    Local ce number(s)     : 0
    Remote ce number(s)    : 0
    Route distinguisher    : 100:2
    MTU                    : 1500
    Import vpn target      : 111:1
    Export vpn target      : 111:1
```

Table 1-13 display mpls l2vpn vpn-name command output description

Field	Description
VPN Name	Name of the VPN
Encap type	Encapsulation type
MTU	Maximum transmission unit
Import vpn target	Incoming VPN target
Export vpn target	Outgoing VPN target

Display information about local CEs of L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1 local-ce
ce-name              ce-id   range   conn-num  LB
ce1                  1       10      0         132096/0/10
LB stands for label block
```

Table 1-14 display mpls l2vpn vpn-name local-ce command output description

Field	Description
ce-name	Name of the CE
ce-id	CE number
range	CE range
conn-num	Number of connections

Field	Description
LB	Label block

Display information about remote CEs of L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1 remote-ce
no.  ce-id peer-id         route-distinguisher     LB
1    4     3.3.3.9         100:1                   132096/0/10
```

Table 1-15 display mpls l2vpn vpn-name remote-ce command output description

Field	Description
no	Sequence number
ce-id	CE ID
peer-id	IP address of the peer
LB	Label block

display mpls l2vpn connection

Syntax

display mpls l2vpn connection [**vpn-name** *vpn-name* [**remote-ce** *ce-id* | **down** | **up** | **verbose**]]

display mpls l2vpn connection [**interface** *interface-type interface-number* | **summary**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-name: VPN name, a case insensitive string of 1 to 31 characters that cannot include the character of “-“.

ce-id: ID of the remote CE for the L2VPN connection, in the range 0 to 249.

down: Displays detailed information about the connections that are down.

up: Displays detailed information about the connections that are up. If you specify neither the **down** nor the **up** keyword, the command displays detailed information about connections that are either up or down.

verbose: Displays detailed information. This keyword is valid only when displaying information about all connections in a VPN.

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

summary: Displays summary information about connections.

Description

Use the **display mpls l2vpn connection** command to display information about Kompella L2VPN connections.

If you do not specify any argument, the command displays information about all Kompella L2VPN connections.

Examples

Display information about all Kompella L2VPN connections.

```
<Sysname> display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
VPN name: vpn1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
  CE name: ce1, id: 1,
  Rid type status peer-id         route-distinguisher   intf
  4   rmt  up     3.3.3.9         100:1                 Vlan2
```

Table 1-16 display mpls l2vpn connection command output description

Field	Description
connections	Statistics about connections, including the number of connections in the state of Up, the number of connections in the state of Down, the number of local connections, the number of remote connections, and the number of unknown connections
VPN name	Name of the VPN
CE name	Name of the CE
id	ID of the CE
Rid	ID of the remote CE
type	Type of the connection
status	Status of the connection
peer-id	IP address of the peer
intf	Interface for the connection

Display information about Kompella L2VPN connections for VPN vpn1.

```
<Sysname> display mpls l2vpn connection vpn-name vpn1
VPN name: vpn1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
  CE name: ce1, id: 1,
  Rid type status peer-id         route-distinguisher   intf
  4   rmt  up     3.3.3.9         100:1                 Vlan2
```

For descriptions of the output fields of the command, see Table 1-16.

Display information about Kompella L2VPN connections on interface Vlan-interface 2.

```
<Sysname> display mpls l2vpn connection interface Vlan-interface 2
```

```
***Conn-type              : remote
   Local vc state         : up
   Remote vc state        : up
   Local ce-id            : 1
   Local ce name          : ce1
   Remote ce-id           : 4
   Intf(state,encap)      : Vlan-interface2 (up,vlan)
   Peer id                : 3.3.3.9
   Route-distinguisher    : 100:1
   Local vc label         : 132100
   Remote vc label        : 132097
   Tunnel policy          : policy1
   Tunnel Type            : lsp
   Tunnel ID              : 0x226013
```

Table 1-17 display mpls l2vpn connection interface command output description

Field	Description
Conn-type	Type of the connection
Local vc state	Local VC status
Remote vc state	Remote VC status
Local ce-id	ID of the local CE
Local ce name	Name of the local CE
Remote ce-id	ID of the remote CE
Intf(state,encap)	Interface name (interface status, interface encapsulation type)
Peer id	IP address of the peer
Local vc label	Local VC label
Remote vc label	Remote VC label
Tunnel policy	Name of the tunneling policy
Tunnel type	Type of the tunnel
Tunnel ID	ID of the tunnel

Display summary information about all Kompella L2VPN connections.

```
<Sysname> display mpls l2vpn connection summary
1 total connections,
connections: 1 up,  0 down , 0 local, 1 remote, 0 unknown
No.   vpn-name    local-num remote-num unknown-num up-num total-num
1     vpn1        0         1          0           1      1
```

Table 1-18 mpls l2vpn connection summary command output description

Field	Description
connections	Statistics about connections, including the number of connections in the state of Up, the number of connections in the state of Down, the number of local connections, the number of remote connections, and the number of unknown connections
No.	Sequence number
vpn-name	Name of the VPN
local-num	Number of local connections
remote-num	Number of remote connections
unknown-num	Number of unknown connections
up-num	Number of connections that are up
total-num	Total number of connections

display mpls l2vpn forwarding-info

Syntax

display mpls l2vpn forwarding-info [*vc-label*] **interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

vc-label: L2VPN VC label, in the range 16 to 4294967295.

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

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

begin: Displays all lines starting with the line that matches the regular expression.

exclude: Displays all lines other than those matching the regular expression..

include: Displays all lines matching the regular expression.

regular-expression: Regular expression, a case-sensitive string of 1 to 80 characters.

Description

Use the **display mpls l2vpn forwarding-info** command to display MPLS L2VPN forwarding information.

Examples

Display MPLS L2VPN forwarding information.

```
<Sysname> display mpls l2vpn forwarding-info interface Vlan-interface 2
```

```
In interface      : Vlan-interface2
Encapsulation type: vlan
MTU               : 1500
Control word      : 1
Entry type        : send
Out VC label      : 8193
Tunnel ID         : 0x110002
```

Table 1-19 display mpls l2vpn forwarding-info command output description

Field	Description
In interface	Incoming interface, which is bound to L2VPN
MTU	Maximum transmission unit
Control word	Whether control word is enabled. 0 means disabled, and 1 means enabled.
Out VC label	Outgoing VC label
Tunnel ID	ID of the public tunnel

display mpls static-l2vc

Syntax

display mpls static-l2vc [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies a CE interface by its type and number.

Description

Use the **display mpls static-l2vc** command to display information about static VCs configured on the router.

If you specify an interface, the command displays only information about static VCs configured on the CE interface.

Examples

Display information about all static VCs configured on the router.

```
<Sysname> display mpls static-l2vc
total connections:  1,  1 up,  0 down
ce-intf         state destination     tr-label  rcv-label tnl-policy
Vlan2            up    3.3.3.9         100       200       policy1
```

Table 1-20 display mpls static-l2vc command output description

Field	Description
total connections	Statistics about connection, including the total number of connections, number of connections that are up, and number of connections that are down
ce-intfe	CE interface
State	Status of the VC
destination	Destination IP address
tr-label	Outgoing label
rcv-label	Incoming label
tnl-policy	Name of the tunneling policy

Display information about static VCs configured on interface Vlan-interface 2.

```
<Sysname> display mpls static-l2vc interface Vlan-interface 2
     ***CE-interface           : Vlan-interface2 is up
        VC State               : up
        Destination            : 3.3.3.9
        Transmit-vpn-label     : 100
        Receive-vpn-label      : 400
        Tunnel Policy          : policy1
        Tunnel Type            : lsp
        Tunnel ID              : 0x226013
```

Table 1-21 display mpls static-l2vc interface command output description

Field	Description
CE-interface	Name of the CE interface
VC State	Status of the VC
Destination	Destination IP address
Transmit-vpn-label	Outgoing label
Receive-vpn-label	Incoming label
Tunnel Policy	Name of the tunneling policy
Tunnel Type	Type of the tunnel
Tunnel ID	ID of the tunnel

l2vpn-family

Syntax

l2vpn-family

undo l2vpn-family

View

BGP view

Default Level

2: System level

Parameters

None

Description

Use the **l2vpn-family** command to enter BGP L2VPN address family view.

Use the **undo l2vpn-family** command to delete all configurations for the BGP L2VPN address family.

Examples

Enter BGP L2VPN address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn]
```

mpls l2vc

Syntax

mpls l2vc *destination vcid* [**tunnel-policy** *tunnel-policy-name*] [**control-word** | **no-control-word**]

undo mpls l2vc

View

Interface view

Default Level

2: System level

Parameters

destination: IP address of the peer PE.

vc-id: VC ID of the L2VPN connection, in the range 1 to 4294967295.

tunnel-policy-name: Tunneling policy for the VC, a string of 1 to 19 characters.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description

Use the **mpls l2vc** command to create a Martini L2VPN connection.

Use the **undo mpls l2vc** command to delete the Martini connection on the CE interface.

- If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number of one.

- At present, the S7900E series Ethernet switches do not support the control word option.

Related commands: **tunnel select-seq load-balance-number** in *MPLS L3VPN Commands* of the *MPLS Volume*.

Examples

Create a Martini MPLS L2VPN connection.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] mpls l2vc 2.2.2.9 999
```

mpls l2vpn

Syntax

mpls l2vpn

undo mpls l2vpn

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **mpls l2vpn** command to enable MPLS L2VPN.

Use the **undo mpls l2vpn** command to disable MPLS L2VPN and delete all L2VPN configurations.

You must use the **mpls l2vpn** command to enable MPLS L2VPN before configuring the other L2VPN commands.

Examples

Enable MPLS L2VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn
```

mpls l2vpn *vpn-name*

Syntax

mpls l2vpn *vpn-name* [**encapsulation** { **ethernet** | **vlan** } [**control-word** | **no-control-word**]]

undo mpls l2vpn *vpn-name*

View

System view, MPLS L2VPN view

Default Level

2: System level

Parameters

vpn-name: Name for the VPN, a case insensitive string of 1 to 31 characters that cannot include the character of "-". It is used to identify a VPN uniquely on a PE.

encapsulation: Specifies the VPN encapsulation type.

ethernet: Uses Ethernet encapsulation.

vlan: Uses VLAN encapsulation.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description

Use the **mpls l2vpn** command to create a Kompella VPN and enter MPLS L2VPN view.

Use the **undo mpls l2vpn** command to delete a VPN.

The encapsulation type specified here must match that of the CE interface.

At present, the S7900E series Ethernet switches do not support the control word option.

Examples

Create Kompella VPN named vpn1 and enter MPLS L2VPN view.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1]
```

Create Kompella VPN named vpn2 and enter MPLS L2VPN view.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] mpls l2vpn vpn2 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn2]
```

mpls static-l2vc destination

Syntax

mpls static-l2vc destination *destination-router-id* **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tunnel-policy-name*] [**control-word** | **no-control-word**]

undo mpls static-l2vc

View

Interface view

Default Level

2: System level

Parameters

dest-router-id: Destination router ID.

transmit-label-value: Outgoing label for the VPN, namely the outgoing label for the static level 2 VC. The value ranges from 16 to 1023.

receive-label-value: Incoming label for the VPN, namely the incoming label for the static level 2 VC. The value ranges from 16 to 1023.

tunnel-policy-name: Tunneling policy for the VC, a string of 1 to 19 characters.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description

Use the **mpls static-l2vc destination** command to create a static VC between CEs connected to different PEs.

Use the **undo mpls static-l2vc** command to delete the static VC.

- You must configure the command on both PEs. The destination address is the IP address of the peer PE. The outgoing label and incoming label are respectively the incoming label and outgoing label of the peer.
- If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number is one.
- At present, the S7900E series Ethernet switches do not support the control word option.

Examples

Create a static VC between CEs connected to different PEs.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 111
receive-vpn-label 222 tunnel-policy pol1
```

mtu (MPLS L2VPN view)

Syntax

mtu *mtu*

undo mtu

View

MPLS L2VPN view

Default Level

2: System level

Parameters

mtu-value: MTU for the L2VPN. It ranges from 128 to 1,500 and defaults to 1,500.

Description

Use the **mtu** command to set the maximum transmission unit (MTU) for the kompella connections.

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

Note

The **mtu** command is not recommended because it affects only negotiation of protocol parameters that may take place and does not affects the forwarding.

Examples

Set the MTU for Kompella connections to 1000.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1
[Sysname-mpls-l2vpn-vpn1] mtu 1000
```

reset bgp l2vpn

Syntax

reset bgp l2vpn { *as-number* | *ip-address* | **all** | **external** | **internal** }

View

User view

Default Level

1: Monitor level

Parameters

as-number: Resets L2VPN BGP connections with the peers in the AS with this number. The AS number must be in the range 1 to 65535.

ip-address: Resets the L2VPN BGP connection to the peer with this IP address.

all: Resets all L2VPN BGP connections.

external: Resets L2VPN EBGP sessions.

internal: Resets L2VPN IBGP sessions.

Description

Use the **reset bgp l2vpn** command to reset L2VPN BGP connections.

Examples

Reset all L2VPN BGP connections.

```
<Sysname> reset bgp l2vpn all
```

route-distinguisher (MPLS L2VPN view)

Syntax

route-distinguisher *route-distinguisher*

View

MPLS L2VPN view

Default Level

2: System level

Parameters

route-distinguisher: Specifies the route distinguisher (RD) in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters.

An RD can be in either of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

Description

Use the **route-distinguisher** command to configure an RD for the VPN.

Different VPNs on a PE must have different RDs, while a VPN can have the same or different RDs on different PEs.

Note

- You cannot change an RD directly; you can only delete the VPN and then re-create the VPN using the new RD.
- No RD is configured by default; you must configure an RD for each VPN. A VPN takes effect only when it is configured with an RD.
- Once you configure an RD for a VPN, you cannot remove the association between the RD and the VPN.

Examples

Configure the RD of a VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 300:1
```

vpn-target (MPLS L2VPN view)

Syntax

vpn-target *vpn-target*&<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | { *vpn-target*&<1-16> [**both** | **export-extcommunity** | **import-extcommunity**] }

View

MPLS L2VPN view

Default Level

2: System level

Parameters

vpn-target: VPN target extended community attributes to be added to the import or export VPN target extended community list, in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters. &<1-16> means that you can specify this argument for up to 16 times.

A VPN target can be in either of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

both: Specifies both the export and import VPN extended communities. This is the default.

export-extcommunity: Specifies the export VPN extended community.

import-extcommunity: Specifies the import VPN extended community.

all: Specifies both the import and export VPN extended communities.

Description

Use the **vpn-target** command to associate a particular VPN with one or more VPN targets.

Use the **undo vpn-target** command to delete the VPN target(s) associated with a particular VPN.

There is no default value for a VPN target. You must configure it when creating the VPN.

Examples

Associate VPN vpn1 with VPN targets.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation vlan
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 300:1
[Sysname-mpls-l2vpn-vpn1] vpn-target 1:1 2:2 export-extcommunity
[Sysname-mpls-l2vpn-vpn1] vpn-target 1.2.3.4:11 import-extcommunity
```

Table of Contents

1 MPLS L3VPN Configuration Commands

Note

For information about BGP L2VPN address family, refer to *MPLS L2VPN Configuration* in the *MPLS Volume*.

MPLS L3VPN Configuration Commands

default local-preference (BGP-VPNv4 subaddress family view)

Syntax

default local-preference *value*

undo default local-preference

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

value: Default value for the local preference, in the range 0 to 4294967295. A greater value represents a higher priority.

Description

Use the **default local-preference** command to set the default value of the local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default value of the local preference is 100.

Examples

With devices A and B connected to the outside AS, configure B with a default local preference of 180 in BGP-VPNv4 subaddress family view, allowing the route going through B to be preferred when more than one route is present.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] default local-preference 180
```

default med (BGP-VPNv4 subaddress family view)

Syntax

default med *med-value*

undo default med

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

med-value: MED value, in the range 0 to 4,294,967,295.

Description

Use the **default med** command to set the default system metric.

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

With other criteria the same, the system selects the route with a smaller MED value as the AS external route.

By default, the MED value is 0.

Examples

Set the default MED to 10 for PE1 in BGP-VPNv4 subaddress family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] default med 10
```

description (VPN instance view)

Syntax

description *text*

undo description

View

VPN instance view

Default Level

2: System level

Parameters

text: Description for the VPN instance, a string of 1 to 80 characters.

Description

Use the **description** command to configure a description for a VPN instance.

Use the **undo description** command to delete the description.

Examples

Configure the description of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] description This is vpn1
```

display bgp vpnv4 all routing-table

Syntax

display bgp vpnv4 all routing-table [*network-address* [{ *mask* | *mask-length* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13> [**no-export-subconfed** | **no-advertise** | **no-export**] * [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **different-origin-as** | **peer** *ip-address* { **advertised-routes** | **received-routes** } [**statistic**] | **regular-expression** *as-regular-expression* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

network-address: IP address of the destination segment.

mask: Network mask, in dotted decimal notation.

mask-length: Length of the network mask, in the range 0 to 32.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays Classless Inter-Domain Routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list in the routing table.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

different-origin-as: Displays information about routes with different AS origins.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Specifies the routing information sent to the specified peer.

received-routes: Specifies the routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS_PATH regular expression.

statistic: Displays BGP VPNv4 route statistics.

Description

Use the **display bgp vpnv4 all routing-table** command to display all BGP VPNv4 routing information.

Examples

Display all BGP VPNv4 routing information.

```
<Sysname> display bgp vpnv4 all routing-table

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 2

 Route Distinguisher: 100:1

    Network            NextHop        In/Out Label      MED        LocPrf

*>i 10.0.0.0           1.1.1.1         1025 /NULL      0          100
*>i 123.1.1.1/32       1.1.1.1         1024 /NULL      0          100

 Total routes of vpn-instance vpn1: 5
    Network            NextHop        In/Out Label      MED        LocPrf

*>i 10.0.0.0           1.1.1.1                         0          100
*>  10.1.1.0/24        0.0.0.0         NULL /1025      0
*>  20.0.0.0           10.1.1.1        NULL /1026      0
*>i 123.1.1.1/32       1.1.1.1                         0          100
*>  124.1.1.1/32       0.0.0.0         NULL /1024      0
```

Display the detailed information of the BGP VPNv4 routes with the prefix being 1.1.1.2 /32.

```
<Sysname> display bgp vpnv4 all routing-table 1.1.1.2 32

 BGP local router ID : 3.3.3.9
 Local AS number : 100


 Route Distinguisher: 100:1
```

```
Paths:   1 available, 1 best

BGP routing table entry information of 1.1.1.2/32:
Label information (Received/Applied): 1034/NULL
From            : 1.1.1.9 (1.1.1.9)
Original nexthop: 1.1.1.9
Ext-Community   : <RT: 111:1>
AS-path         : 65410
Origin          : incomplete
Attribute value : MED 0, localpref 100, pref-val 0, pre 255
State           : valid, internal, best,
Not advertised to any peers yet


Total Number of Routes: 1(vpna)
Paths:   1 available, 1 best

BGP routing table entry information of 1.1.1.2/32:
From            : 1.1.1.9 (1.1.1.9)
Relay Nexthop   : 0.0.0.0
Original nexthop: 1.1.1.9
Ext-Community   : <RT: 111:1>
AS-path         : 65410
Origin          : incomplete
Attribute value : MED 0, localpref 100, pref-val 0, pre 255
State           : valid, internal, best,
Not advertised to any peers yet

Not advertised to any VPNv4 peers yet
```

Table 1-1 display bgp vpnv4 all routing-table output description

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. Valid values include: * - valid: Valid route > - best: Best route d - damped: Route damped for route flap h - history: History route i - internal: Internal route s - suppressed: Suppressed route S - Stale: Stale route
Origin	Route origin codes. Valid values include: i - IGP (learned from within the AS) e - EGP (learned through EGP) ? - incomplete (learned in any other way)
Total number of routes from all PE	Total number of VPNv4 routes from all PEs

Field	Description
Network	Network address
NextHop	Address of the next hop
In/Out Label	Incoming and outgoing labels
MED	Metric associated with the destination network
Total routes of vpn-instance vpn1	Total number of routes of the specified VPN instance
LocPrf	Local preference
Paths	Counts of routes, including: • available: Number of available routes. • best: Number of best routes
Label information	Route label information • Received: Received label information • Applied: Locally generated label information
Ext-Community	Extended community attribute
AS-path	The route's AS path attribute (AS_PATH), which records all ASs the route has passed, and therefore can avoid route loops.
Attribute value	BGP routing attribute information
localpref	Local precedence
pref-val	Preferred value
pre	Protocol priority
State	Route status, which can be: • valid: Valid route • internal: Internal route • external: External route • local: Locally generated route • synchronize: Synchronized route • best: Best route

display bgp vpnv4 group

Syntax

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

Description

Use the **display bgp vpnv4 group** command to display information about a specified or all BGP VPNv4 peer groups.

Examples

Display information about BGP VPNv4 peer group a for VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 group a

 BGP peer-group is a
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 99
 No routing policy is configured
  Members:
  Peer        V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State
  10.1.1.1    4   200   18       21     0     1      00:12:58 Established
```

Table 1-2 display bgp vpnv4 group command output description

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS number	Number of the remote AS
Type	Type of the BGP peer group
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Configured hold timer value	Setting of the hold timer
Keepalive timer value	Keepalive interval
Peer Preferred Value	Weight for the routes from the peer
No routing policy is configured	Whether the VPN instance is configured with a routing policy
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer

Field	Description
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

display bgp vpnv4 network

Syntax

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **network**

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description

Use the **display bgp vpnv4 network** command to display information about BGP VPNv4 routes injected into a specified or all VPN instances.

Examples

Display information about BGP VPNv4 routes injected into VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 network
  BGP Local Router ID is 1.1.1.1.
  Local AS Number is 100.
  Network          Mask            Route-policy
  10.0.0.0         255.0.0.0
```

Table 1-3 display bgp vpnv4 network command output description

Field	Description
BGP Local Router ID	Router ID of the local BGP router
Network	Advertised network route
Mask	Mask of the advertised network route
Route-policy	Routing policy configured

display bgp vpnv4 paths

Syntax

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

as-regular-expression: Regular expression for filtering the AS path information to be displayed.

Description

Use the **display bgp vpnv4 paths** command to display the BGP VPNv4 AS path information.

Examples

Display the BGP VPNv4 AS path information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 paths

    Address       Hash    Refcount  MED         Path/Origin
    0x6E72D18     0       1           0           200?
    0x6E72E50     0       1           0           i
    0x6E72B78     1       1           0           ?
    0x6E72BE0     1       2           0           ?
```

Display all BGP VPNv4 AS path information.

```
<Sysname> display bgp vpnv4 all paths

    Address       Hash    Refcount  MED         Path/Origin
    0x6E72D80     4       1         0           200?
    0x6E72CB0     15      2         0           ?
```

Table 1-4 display bgp vpnv4 paths command output description

Field	Description
Address	Routing address in the local database
Hash	Hash bucket for storing routes
Refcount	Number of times that the path is referenced
MED	Metric for routes
Path/Origin	AS_PATH and origin attributes of the route, see Table 1-1.

display bgp vpnv4 peer

Syntax

display bgp vpnv4 all peer [*ip-address* **verbose** | **verbose**]

display bgp vpnv4 vpn-instance *vpn-instance-name* **peer** [*group-name* **log-info** | *ip-address* { **log-info** | **verbose** } | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

log-info: Displays log information.

ip-address: IP address of the peer.

verbose: Displays detailed information.

Description

Use the **display bgp vpnv4 peer** command to display information about BGP VPNv4 peers.

Examples

Display information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer
 BGP local router ID : 2.2.2.2
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

 Peer         V   AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down  State
 10.1.1.1     4   200    24       29       0       1      00:18:47 Established
```

Table 1-5 display bgp vpnv4 vpn-instance peer output description

Field	Description
BGP Local router ID	Router ID of the local BGP router
Peers in established state	Number of peers in the state of established
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent

Field	Description
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of received prefixes
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer verbose

          Peer: 10.1.1.1  Local: 2.2.2.2
          Type: EBGP link
          BGP version 4, remote router ID 10.1.1.1
          BGP current state: Established, Up for 00h19m26s
          BGP current event: KATimerExpired
          BGP last state: OpenConfirm
          Port:  Local - 179      Remote - 1025
          Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
          Received  : Active Hold Time: 180 sec
          Negotiated: Active Hold Time: 180 sec
          Peer optional capabilities:
          Peer support bgp multi-protocol extended
          Peer support bgp route refresh capability
          Address family IPv4 Unicast: advertised and received

 Received: Total 25 messages, Update messages 1
 Sent: Total 30 messages, Update messages 4
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
Nesting-vpn peer (vpn-instance vrf1) has been configured
 Peer Preferred Value: 99

Routing policy configured:
 No routing policy is configured
```

Table 1-6 display bgp vpnv4 peer verbose output description

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router

Field	Description
BGP current state	Current status of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current status
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Received	Counts of received messages and received update messages
Sent	Counts of sent messages and sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Optional capabilities	Local optional capabilities
Route refresh capability has been enabled	Whether the route refresh capability is supported
Nesting-vpn peer (vpn-instance vrf1)	Whether the VPNv4 peer is a nested VPN peer
Peer Preferred Value	Weight for the routes from the peer

Display all BGP VPNv4 peer information.

```
<Sysname> display bgp vpnv4 all peer

 BGP local router ID : 2.2.2.2
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

  Peer     V   AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down   State
  1.1.1.1  4  100   51       64        0     2      00:45:16  Established
```

Table 1-7 display bgp vpnv4 all peer command output description

Field	Description
Peer	IP address of the peer
V	Version of BGP that the peer runs

Field	Description
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peer 1.1.1.1.

```
<Sysname> display bgp vpnv4 all peer 1.1.1.1 verbose
         Peer: 1.1.1.1   Local: 2.2.2.2
         Type: IBGP link
         BGP version 4, remote router ID 1.1.1.1
         BGP current state: Established, Up for 00h46m01s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 1039     Remote - 179
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer support bgp multi-protocol extended
         Peer support bgp route refresh capability
         Address family IPv4 Unicast: advertised and received
         Address family VPNv4: advertised and received
 Received: Total 52 messages, Update messages 2
 Sent: Total 65 messages, Update messages 5
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 15 seconds
 Optional capabilities:
 Route refresh capability has been enabled
Nesting-vpn peer (vpn-instance vrf1) has been configured
 Connect-interface has been configured
 Peer Preferred Value: 0

 Routing policy configured:
 No routing policy is configured
```

Table 1-8 display bgp vpnv4 all peer verbose output description

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type

Field	Description
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router
BGP current state	Current status of BGP
Up for	Duration since the peer is established
BGP current event	Current event of the peer
BGP last state	State that BGP was in before transitioning to the current status
Port	Local and remote BGP port numbers
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Address family VPNv4	IPv4 address group VPNv4 capability
Received	Counts of received messages and received update messages
Sent	Counts of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Optional capabilities	Local optional capabilities
Route refresh capability	Whether the route refresh capability is supported
Nesting-vpn peer (vpn-instance vrf1)	Whether the VPNv4 peer is a nested VPN peer
Connect-interface	Whether a source interface is configured for route update messages
Peer Preferred Value	Weight configured for routes from the peer

Display the log information of BGP VPNv4 peer whose address is 1.1.1.1.

```
<sysname> display bgp vpnv4 vpn-instance vpn1 peer 1.1.1.1 log-info

 Peer : 1.1.1.1

     Date      Time    State Notification
                             Error/SubError

  10-Jul-2008 15:46:17 Down  Send Notification with Error 1/1
                             Message Header Error/Connection Not Synchronized
```

```
10-Jul-2008 09:23:00 Up
10-Jul-2008 07:46:17 Down  Receive Notification with Error 3/2
                           UPDATE Message Error/Unsupported optional Parameter
10-Jul-2008 06:23:00 Up
10-Jul-2008 05:46:17 Down  Send Notification with Error 6/4
                           Administrative Reset
```

Table 1-9 display bgp vpnv4 peer log-info command output description

Field	Description
Peer	IPv4 address of the peer
Date	Date when the notification message is sent or received
Time	Time when the notification message is sent or received
State	Connection state of the peer, which can be: • Up: The BGP session is in the Established state. • Down: The BGP session has been cut down.
Notification	Notification message
Error/SubError	Error: Notification message error code, which specifies the error type.
	SubError: Notification message's error subcode, which specifies the detailed information of the error.

display bgp vpnv4 route-distinguisher routing-table

Syntax

display bgp vpnv4 route-distinguisher *route-distinguisher* **routing-table** [*network-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13> [**no-export-subconfed** | **no-advertise** | **no-export**] * [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **different-origin-as** | **regular-expression** *as-regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

route-distinguisher: Route distinguisher (RD).

network-address: IP address of the destination segment.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays Classless Interdomain Routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact matching.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

different-origin-as: Displays information about routes with different AS origins.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

Description

Use the **display bgp vpnv4 route-distinguisher routing-table** command to display the BGP VPNv4 routing information of a specified RD.

Related commands: **route-distinguisher**.

Examples

Display the BGP VPNv4 routing information of RD 100:1.

```
<Sysname> display bgp vpnv4 route-distinguisher 100:1 routing-table

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1
 Total number of routes: 2

    Network            NextHop         In/Out Label   MED        LocPrf

*>i 10.0.0.0           1.1.1.1         1025 /NULL      0          100
*>i 123.1.1.1/32       1.1.1.1         1024 /NULL      0          100

 Total routes of vpn-instance vpn1: 5
    Network            NextHop         In/Out Label   MED        LocPrf

*>i 10.0.0.0           1.1.1.1                         0          100
*>  10.1.1.0/24        0.0.0.0         NULL /1025      0
*>  20.0.0.0           10.1.1.1        NULL /1026      0
```

```
*>i 123.1.1.1/32       1.1.1.1                         0          100
*>  124.1.1.1/32       0.0.0.0         NULL /1024      0
```

Display the BGP VPNv4 routing information with the RD being 100:1 and IP address being 1.1.1.2.

```
<Sysname> display bgp vpnv4 route-distinguisher 100:1 routing-table 1.1.1.2 32

 BGP local router ID : 3.3.3.9
 Local AS number : 100


 Route Distinguisher: 100:1
 Paths:   1 available, 1 best

 BGP routing table entry information of 1.1.1.2/32:
 Label information (Received/Applied): 1034/NULL
 From            : 1.1.1.9 (1.1.1.9)
 Original nexthop: 1.1.1.9
 Ext-Community   : <RT: 111:1>
 AS-path         : 65410
 Origin          : incomplete
 Attribute value : MED 0, localpref 100, pref-val 0, pre 255
 State           : valid, internal, best,
 Not advertised to any peers yet


 Total Number of Routes: 1(vpna)
 Paths:   1 available, 1 best

 BGP routing table entry information of 1.1.1.2/32:
 From            : 1.1.1.9 (1.1.1.9)
 Relay Nexthop   : 0.0.0.0
 Original nexthop: 1.1.1.9
 Ext-Community   : <RT: 111:1>
 AS-path         : 65410
 Origin          : incomplete
 Attribute value : MED 0, localpref 100, pref-val 0, pre 255
 State           : valid, internal, best,
 Not advertised to any peers yet
```

The following table gives the description on the fields of the **display bgp vpnv4 route-distinguisher routing-table** command.

Table 1-10 Output description

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. For valid values, see Table 1-1.
Origin	Route origin codes. For valid values, see Table 1-1.
Network	Network address

Field	Description
NextHop	Address of the next hop
In/Out Label	Incoming/outgoing label
MED	Metric associated with the destination network
LocPrf	Local preference
Total routes of vpn-instance vpn1	Total number of routes of the specified VPN instance
Paths	Counts of routes, including: • available: Number of available routes. • best: Number of best routes
Label information	Route label information • Received: Received label information • Applied: Locally generated label information
Ext-Community	Extended community attribute
AS-path	The route's AS path attribute (AS_PATH), which records all ASs the route has passed, and therefore can avoid route loops.
Attribute value	BGP routing attribute information
localpref	Local precedence
pref-val	Preferred value
pre	Protocol priority
State	Current state of the peer, which can be: • valid • internal • best

Display the BGP VPNv4 routing information with RD being 100:1 and the network segment address being 10.0.0.0.

```
<Sysname> display bgp vpnv4 route-distinguisher 100:1 routing-table 10.0.0.0 255.0.0.0

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1
 Total number of routes: 1

    Network            NextHop         In/Out Label   MED        LocPrf

*>i 10.0.0.0           1.1.1.1         1025 /NULL      0          100

 Total Number of Routes: 1(vpn1)
    Network            NextHop         In/Out Label   MED        LocPrf

*>i 10.0.0.0           1.1.1.1                          0          100
```

The following table gives the description on the fields of the **display bgp vpnv4 route-distinguisher routing-table** command.

Table 1-11 Output description

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. For valid values, see Table 1-1.
Origin	Route origin codes. For valid values, see Table 1-1.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
In/Out Label	Incoming/outgoing label
MED	Metric associated with the destination network
LocPrf	Local preference
Total Number of Routes	Total number of routes of the specified VPN instance

display bgp vpnv4 routing-table label

Syntax

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table label**

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description

Use the **display bgp vpnv4 routing-table label** command to display information about labeled routes in the BGP routing table.

Examples

Display information about labeled routes in the BGP routing table.

```
<Sysname> display bgp vpnv4 all routing-table label

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
Total number of routes from all PE: 1

Route Distinguisher: 100:1

       Network          NextHop          In/Out Label
*>i    123.1.1.1        1.1.1.1          NULL/1024

Total routes of vpn-instance vpn1: 4

       Network          NextHop          In/Out Label
*>     10.1.1.0         0.0.0.0          1025/NULL
*>     20.0.0.0         0.0.0.0          1026/NULL
*>i    123.1.1.1        1.1.1.1          NULL/1024
*>     124.1.1.1        0.0.0.0          1024/NULL
```

Table 1-12 display bgp vpnv4 routing-table label output description

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status	Route status codes. For valid values, see Table 1-1.
Origin	Route origin codes. For valid values, see Table 1-1.
Route Distinguisher	RD
Network	Network address
NextHop	Address of the next hop
In/Out Label	Incoming/outgoing label. exp-null indicates an explicit null label.
Total routes of vpn-instance vpn1	Total number of routes from the specified VPN instance

display bgp vpnv4 vpn-instance routing-table

Syntax

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table** [*network-address* [{ *mask* | *mask-length* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13>[**no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **dampened** | **dampening parameter** | **different-origin-as** | **flap-info** [**as-path-acl** *as-path-acl-number* | *network-address* [*mask* [**longer-match**] | *mask-length* [**longer-match**]] | **regular-expression** *as-regular-expression*] | **peer** *ip-address* { **advertised-routes** | **received-routes** } | **regular-expression** *as-regular-expression* | **statistic**]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

network-address: IP address of the destination segment.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays Classless Interdomain Routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

dampened: Displays information about dampened BGP VPNv4 routes.

dampening parameter: Displays information about configured BGP VPNv4 route dampening parameters.

different-origin-as: Displays information about routes with different AS origins.

flap-info: Displays BGP VPNv4 route flap statistics.

longer-match: Displays flap statistics for routes with masks longer than that specified by the *network-address* { *mask* | *mask-length* } combination.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Displays routing information sent to the specified peer.

received-routes: Displays routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

statistic: Displays BGP VPNv4 route statistics.

Description

Use the **display bgp vpnv4 vpn-instance routing-table** command to display the BGP VPNv4 routing information of a specified VPN instance.

Examples

Display the BGP VPNv4 routing information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 routing-table

 Total Number of Routes: 5

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Network            NextHop         MED        LocPrf    PrefVal Path/Ogn

 *>i 10.0.0.0       1.1.1.1         0          100        0       i
 *>  10.1.1.0/24    0.0.0.0         0                     0       ?
 *>  20.0.0.0       10.1.1.1        0                     99      200?
 *>i 123.1.1.1/32   1.1.1.1         0          100        0       ?
 *>  124.1.1.1/32   0.0.0.0         0                     0       ?
```

The following table gives the description on the fields of the **display bgp vpnv4 vpn-instance routing-table** command.

Table 1-13 Output description

Field	Description
BGP Local router ID	ID of the BGP-enabled local router
Status codes	Route status codes. For valid values, see Table 1-1.
Origin	Route origin codes. For valid values, see Table 1-1.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
MED	Metric associated with the destination network
LocPrf	Local preference
PrefVal	Preferred value of the protocol
Path/Ogn	AS_PATH attribute/route origin of the route, see Table 1-1.

display fib statistics vpn-instance

Syntax

display fib statistics vpn-instance

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display fib statistics vpn-instance** command to display the FIB information of the VPN instances.

Examples

View statistics about the FIB entries.

```
<Sysname> display fib statistics vpn-instance
Route Entry Count          : 10
```

Table 1-14 display fib statistics vpn-instance command output description

Field	Description
Route Entry Count	Number of the route entries of all the VPN instances

display fib vpn-instance

Syntax

display fib vpn-instance *vpn-instance-name* [**include** *string*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

include: Displays the lines that include the specified string.

string: String for matching against the information to be displayed. It is case sensitive and consists of 1 to 256 characters.

Description

Use the **display fib vpn-instance** command to display the FIB information of a VPN instance.

Examples

Display all FIB information of VPN instance **vpn1**.

```
<Sysname> display fib vpn-instance vpn1
<Sysname> display fib vpn-instance vpn1
FIB Table For vpn1:
 Total number of Routes : 2
Destination/Mask    OutInterface                 InnerLabel     Token
66.1.1.1/32         InLoopBack0                  NULL           invalid
66.1.1.0/24         InLoopBack0                  NULL           invalid
```

Table 1-15 display fib vpn-instance command output description

Field	Description
FIB entry count	Number of entries in the FIB
Destination/Mask	Destination address/mask length
OutInterface	Forwarding interface
Token	LSP index number

display ip vpn-instance

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

View

Any view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description

Use the **display ip vpn-instance** command to display information about a VPN instance or all VPN instances.

If you do not specify any parameter, the command displays brief information about all VPN instances.

Examples

Display information about all VPN instances.

```
<Sysname> display ip vpn-instance
  Total VPN-Instances configured : 2

  VPN-Instance Name      RD          Create Time
  vpn1                  22:1         2003/10/13 09:32:45
  vpn2                  33:3         2003/10/13 09:42:59
```

Table 1-16 display ip vpn-instance command output description

Field	Description
VPN-Instance Name	Name of the VPN instance
RD	RD of the VPN instance
Create Time	Time when the VPN instance was created

Display detailed information about a VPN instance.

```
<Sysname> display ip vpn-instance instance-name vpn1
```

```
VPN-Instance Name and ID : vpn1, 1
Create time : 2006/04/08 13:01:30
Up time : 0 days, 00 hours, 11 minutes and 42 seconds
Route Distinguisher : 22:1
Export VPN Targets :  3:3 5:5
Import VPN Targets :  4:4 5:5
Import Route Policy : poly-1
Description : This is vpn1
Maximum number of Routes : 500
Interfaces :  Vlan-interface10
```

Table 1-17 display ip vpn-instance instance-name output description

Field	Description
VPN-Instance Name and ID	Name and ID of the VPN instance
CreateTime	Time when the VPN instance was created
Up time	Duration of the VPN instance
Route Distinguisher	RD of the VPN instance
Export VPN Targets	Export target attribute of the VPN instance
Import VPN Targets	Import target attribute of the VPN instance
Import Route Policy	Import routing policy of the VPN instance
Description	Description of the VPN instance
Maximum number of Routes	Maximum number of routes of the VPN instance
Interfaces	Interface to which the VPN instance is bound

display ospf sham-link

Syntax

display ospf [*process-id*] **sham-link** [**area** *area-id*]

View

Any view

Default Level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range 1 to 65535.

area-id: OSPF area ID. It can be an integer in the range 0 to 4294967295 or in the format of an IPv4 address.

Description

Use the **display ospf sham-link** command to display information about sham links.

With neither process ID nor area ID specified, the command displays information about all configured sham links.

Related commands: **sham-link**.

Examples

Display information about all OSPF sham links.

```
<Sysname> display ospf sham-link
          OSPF Process 100 with Router ID 100.1.1.2
 Sham Link:
 Area        RouterId     Source-IP     Destination-IP  State Cost
 0.0.0.1     100.1.1.2    3.3.3.3       5.5.5.5         P-2-P 10
```

Table 1-18 display ospf sham-link command output description

Field	Description
Area	OSPF area to which the sham link belongs
RouterId	Router ID of the sham link
Source-IP	Source IP address of the sham link
Destination-IP	Destination IP address of the sham link
State	Status of the sham link interface
Cost	Cost of the sham link

Display information about OSPF sham links in area 1.

```
<Sysname> display ospf sham-link area 1
          OSPF Process 100 with Router ID 100.1.1.2
  Sham-Link: 3.3.3.3 --> 5.5.5.5
  Neighbour State: Full
  Area: 0.0.0.1
  Cost: 10  State: P-2-P, Type: Sham
  Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 1-19 display ospf sham-link area command output description

Field	Description
Sham-Link	Sham link expressed in the format of source IP address to destination IP address
Neighbour State	Status of the sham link neighbor
Area	Destination IP address of the sham link
Cost	Cost of the sham link
State	Status of the sham link
Type	Type of the sham link
Timers	Timers of the sham link

display tunnel-policy

Syntax

display tunnel-policy { **all** | **policy-name** *tunnel-policy-name* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all tunneling policies.

tunnel-policy-name: Name of a tunneling policy, a string of 1 to 19 characters.

Description

Use the **display tunnel-policy** command to display information about a tunneling policy or all tunneling policies.

Related commands: **tunnel-policy**, **tunnel select-seq load-balance-number**.

Examples

Display all tunneling policies.

```
<Sysname>display tunnel-policy all
Tunnel Policy Name   Select-Seq       Load balance No
-----------------------------------------------------
t                    LSP              1
bbb                  LSP              1
```

Display tunneling policy aaa.

```
<Sysname>display tunnel-policy policy-name aaa
Tunnel Policy Name   Select-Seq       Load balance No
-----------------------------------------------------
aaa                  LSP              1
```

Table 1-20 display tunnel-policy command output description

Field	Description
Tunnel Policy Name	Name of the tunneling policy
Select-Seq	preference order for tunnel selection
Load balance No	Number of tunnels for load balancing

domain-id

Syntax

domain-id *domain-id* [**secondary**]

undo domain-id [*domain-id*]

View

OSPF view

Default Level

2: System level

Parameters

domain-id: OSPF domain ID, in integer or dotted decimal notation. If it is in integer, it ranges from 0 to 4,294,967,295.

secondary: Uses the domain ID as secondary. With this keyword not specified, the domain ID configured is primary.

Description

Use the **domain-id** command to configure an OSPF domain ID.

Use the **undo domain-id** command to restore the default.

By default, the OSPF domain ID is 0.

With no parameter specified, the **undo domain-id** command deletes all domain IDs.

Usually, routes injected from PEs are advertised as External-LSAs. However, routes to different destinations in the same OSPF domain must be advertised as Type-3 LSAs. Therefore, using the same domain ID for an OSPF domain is required.

Examples

Configure the OSPF domain ID.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] domain-id 234
```

export route-policy

Syntax

export route-policy *route-policy*

undo export route-policy

View

VPN instance view

Default Level

2: System level

Parameters

route-policy: Name of the export routing policy for the VPN instance, a string of 1 to 19 characters.

Description

Use the **export route-policy** command to apply an export routing policy to a VPN instance.

Use the **undo export route-policy** command to remove the application.

You can configure an export routing policy when a finer control on the VPN instance routes to be redistributed is required, that is, when the control provided by the extended community attribute is not enough. An export routing policy may deny routes that are permitted by the export target attribute.

By default, all VPN instance routes permitted by the export target attribute can be redistributed.

Examples

Apply export routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

ext-community-type

Syntax

ext-community-type { **domain-id** *type-code1* | **router-id** *type-code2* | **route-type** *type-code3* }

undo ext-community-type { **domain-id** | **router-id** | **route-type** }

View

OSPF view

Default Level

2: System level

Parameters

domain-id *type-code1*: Specifies the type code for the OSPF extended community attribute of Domain ID. Valid values are 0x0005, 0x0105, 0x0205, and 0x8005.

router-id *type-code2*: Specifies the type code for the OSPF extended community attribute of Router ID. Valid values are 0x0107 and 0x8001.

router-type *type-code3*: Specifies the type code for the OSPF extended community attribute of Route Type. Valid values are 0x0306 and 0x8000.

Description

Use the **ext-community-type** command to configure the type code of an OSPF extended community attribute.

Use the **undo ext-community-type** command to restore the default.

By default, the type codes for the OSPF extended community attributes of Domain ID, Router ID, and Route Type are 0x0005, 0x0107, and 0x0306 respectively.

Examples

Configure the type codes of OSPF extended community attributes Domain ID, Router ID, and Route Type as 0x8005, 0x8001, and 0x8000 respectively for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ext-communityroute-type domain-id 8005
[Sysname-ospf-100] ext-communityroute-type router-id 8001
[Sysname-ospf-100] ext-communityroute-type route-type 8000
```

filter-policy export (BGP-VPNv4 subaddress family view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

acl-number: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

direct: Filters direct routes to be advertised.

isis *process-id*: Filters ISIS routes to be advertised that are from a specified ISIS process. The *process-id* argument is in the range 1 to 65535.

ospf *process-id*: Filters OSPF routes to be advertised that are from a specified OSPF process. The *process-id* argument is in the range 1 to 65535.

rip *process-id*: Filters RIP routes to be advertised that are from a specified RIP process. The *process-id* argument is in the range 1 to 65535.

static: Filters static routes to be advertised.

Description

Use the **filter-policy export** command to specify to filter all or certain types of routes to be advertised.

Use the **undo filter-policy export** command to remove the configuration.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised will be filtered.

By default, MP-BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by MP-BGP.

Examples

In BGP-VPNv4 subaddress family view, specify to filter routes to be advertised by MP-BGP using ACL 2555.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] filter-policy 2555 export
```

filter-policy import (BGP-VPNv4 subaddress family view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

acl-number: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

Description

Use the **filter-policy import** command to specify to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

By default, received routes are not filtered.

Only routes that survive the filtering are added into the BGP routing table.

Examples

In BGP-VPNv4 subaddress family view, specify to use ACL 2255 to filter received routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] filter-policy 2255 import
```

import route-policy

Syntax

import route-policy *route-policy*

undo import route-policy

View

VPN instance view

Default Level

2: System level

Parameters

route-policy: Name of the import routing policy for the VPN instance, a string of 1 to 19 characters.

Description

Use the **import route-policy** command to apply an import routing policy to a VPN instance.

Use the **undo import route-policy** command to remove the application.

You can configure an import routing policy when a finer control on the routes to be redistributed into a VPN instance is required, that is, when the control provided by the extended community attributes is not enough. An import routing policy may deny routes that are permitted by the import target attribute.

By default, all routes permitted by the import target attribute can be redistributed into the VPN instance.

Examples

Apply import routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1
```

ip binding vpn-instance

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

View

Interface view

Default Level

2: System level

Parameters

vpn-instance-name: Name of the VPN instance to be associated, a case-insensitive string of 1 to 31 characters.

Description

Use the **ip binding vpn-instance** command to associate an interface with a VPN instance.

Use the **undo ip binding vpn-instance** command to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must re-configure the IP address of the interface after configuring the command.

Examples

Associate interface VLAN-interface 1 with VPN instance vpn1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1
```

ip vpn-instance

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

View

System view

Default Level

2: System level

Parameters

vpn-instance-name: Name for the VPN instance, a case-sensitive string of 1 to 31 characters.

Description

Use the **ip vpn-instance** command to create a VPN instance and enter VPN instance view.

Use the **undo ip vpn-instance** command to delete a VPN instance.

A VPN instance takes effect only after you configure an RD for it.

Related commands: **route-distinguisher**.

Examples

Create a VPN instance named vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

ipv4-family

Syntax

ipv4-family { **vpnv4** | **vpn-instance** *vpn-instance-name* }

undo ipv4-family { **vpnv4** | **vpn-instance** *vpn-instance-name* }

View

BGP view

Default Level

2: System level

Parameters

vpnv4: Enters BGP-VPNv4 subaddress family view.

vpn-instance *vpn-instance-name*: Associates a VPN instance with an IPv4 address family and enter BGP VPN instance view. The *vpn-instance-name* argument is a string of 1 to 31 characters.

Description

Use the **ipv4-family** command to enter BGP-VPNv4 subaddress family view or BGP VPN instance view.

Use the **undo ipv4-family** command to remove all configurations performed in either of the two views.

Before entering BGP VPN instance view, you must create the VPN instance.

Examples

Enter BGP-VPNv4 subaddress family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4]
```

Associate VPN instance vpn1 with an IPv4 address family and enter BGP VPN instance view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] quit
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1]
```

nesting-vpn

Syntax

nesting-vpn

undo nesting-vpn

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

None

Description

Use the **nesting-vpn** command to enable the nested VPN function.

Use the **undo nesting-vpn** command to disable the nested VPN function.

By default, the nested VPN function is disabled.

If a nested VPN peer connected to a PE needs to advertise VPNv4 routes, you need to enable nested VPN on the PE.

Examples

Enable nested VPN.

```
<Sysname> system-view
[Sysname] bgp 10
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] nesting-vpn
```

peer advertise-community (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer advertise-community** command to specify to advertise community attributes to a peer or peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attributes are advertised to any peer or peer group.

Examples

In BGP-VPNv4 subaddress family view, specify to advertise community attributes to peer 3.3.3.3.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 3.3.3.3 advertise-community
```

peer allow-as-loop

Syntax

peer { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

number: Maximum number that the local AS number can appear repeatedly in the AS-PATH attribute. It ranges from 1 to 10 and defaults to 1.

Description

Use the **peer allow-as-loop** command to allow the local AS number to appear in the AS-PATH attribute of a received route and to set the allowed maximum number of repetitions.

Use the **undo peer allow-as-loop** command to remove the configuration.

Examples

In BGP-VPNv4 subaddress family view, allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 allow-as-loop 2
```

In BGP-L2VPN address family view, allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 allow-as-loop 2
```

peer as-path-acl (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

as-path-acl-number: AS_PATH filtering list number, in the range 1 to 256.

import: Filters the received routes.

export: Filters the routes to be advertised.

Description

Use the **peer as-path-acl** command to specify to filter routes received from or to be advertised to a specified peer or peer group based on an AS_PATH list.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS filtering list is applied to a peer or peer group.

Examples

In BGP-VPNv4 subaddress family view, apply AS filtering list 3 to routes advertised by peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test as-path-acl 3 export
```

peer default-route-advertise vpn-instance

Syntax

peer { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*

undo peer { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description

Use the **peer default-route-advertise vpn-instance** command to specify to advertise all default routes of a VPN instance to a peer or peer group.

Use the **undo peer default-route-advertise vpn-instance** command to remove the configuration.

By default, no default route is advertised to a peer or peer group.

Related commands: **peer upe**.

Examples

In BGP-VPNv4 subaddress family view, specify to advertise default routes of VPN instance vpn1 to peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 enable
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 default-route-advertise vpn-instance vpn1
```

peer enable

Syntax

peer { *group-name* | *ip-address* } **enable**

undo peer { *group-name* | *ip-address* } **enable**

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer enable** command to enable a peer or peer group for an address family and enable the exchange of BGP routing information of the address family.

Use the **undo peer enable** command to disable the capability.

By default, only IPv4 routing information is exchanged between BGP peers/peer groups.

Examples

Configure peer 1.1.1.1 and enable the peer for the BGP-VPNv4 subaddress family.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 enable
```

Configure peer 1.1.1.1 and enable the peer for the BGP-L2VPN address family.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 enable
```

peer filter-policy (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description

Use the **peer filter-policy** command to apply a filtering policy to a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no filtering policy is applied to a peer or peer group.

Related commands: **peer as-path-acl**.

Examples

Apply a filtering policy to filter the received routes of a peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test filter-policy 2003 import
```

peer group

Syntax

peer *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

as-number *as-number*: Specifies an AS number, which ranges from 1 to 65535.

Description

Use the **peer group** command to add a peer into an existing peer group.

Use the **undo peer group** command to remove a peer from a peer group.

Examples

In BGP-VPNv4 subaddress family view, add peer 1.1.1.1 into peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 group test
```

In BGP-L2VPN address family view, add peer 1.1.1.1 into peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 group test
```

peer ip-prefix (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **ip-prefix** *prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** *prefix-name* { **export** | **import** }

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

prefix-name: Name of the IP prefix list, a string of 1 to 19 characters.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description

Use the **peer ip-prefix** command to apply a route filtering policy based on IP prefix list to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no route filtering policy based on IP prefix list is applied to a peer or peer group.

Examples

In BGP-VPNv4 subaddress family view, specify to filter the received routes of a peer group using IP prefix list list1.

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer group1 ip-prefix list1 import
```

peer label-route-capability (BGP view, BGP VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **label-route-capability**

undo peer { *group-name* | *ip-address* } **label-route-capability**

View

BGP view, BGP VPN instance view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer label-route-capability** command to enable the exchange of labeled routes with an IPv4 peer or peer group.

Use the **undo peer label-route-capability** command to disable the capability.

By default, the device does not advertise labeled routes to an IPv4 peer.

According to the networking scheme, the **peer label-route-capability** command enables the exchange of labeled IPv4 routes with:

- ASBR PEs in the same AS.
- PEs in the same AS.
- the peer ASBR PE.

Examples

Specify to exchange labeled IPv4 routes with peer 2.2.2.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 2.2.2.2 label-route-capability
```

peer next-hop-invariable (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **next-hop-invariable**

undo peer { *group-name* | *ip-address* } **next-hop-invariable**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer next-hop-invariable** command to configure the device not to change the next hop of a route when advertising it to a peer.

Use the **undo peer next-hop-invariable** command to restore the default.

By default, a device uses its address as the next hop when advertising a route to its EBGP peer. In the inter-provider option C application, you need to configure **next-hop-invariable** on the RR for multi-hop EBGP neighbors and reflector clients to ensure that the next hop of a VPN route will not be changed.

Related commands: **peer ebgp-max-hop** in *BGP Commands* of the *IP Routing Volume*.

Examples

In BGP-VPNv4 subaddress family view, configure the device not to change the next hop of a route when advertising it to EBGP peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 next-hop-invariable
```

peer next-hop-local

Syntax

peer { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer next-hop-local** command to configure the device to use the local address as the next hop of a route when advertising it to a peer or peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

Examples

In BGP-VPNv4 subaddress family view, configure the device to use the local address as the next hop of a route when advertising it to peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test next-hop-local
```

In BGP-L2VPN address family view, configure the device to use the local address as the next hop of a route when advertising it to peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer test next-hop-local
```

peer preferred-value (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

value: Preferred value to be specified, in the range 0 to 65535.

Description

Use the **peer preferred-value** command to specify the preferred value for the routes received from the specified peer/peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, the preferred value for the routes received from a peer/peer group is 0.

Examples

Set the preferred value for the routes received from peer 131.108.1.1 to 50.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer public-as-only** command to make outbound BGP updates carry no private AS numbers.

Use the **undo peer public-as-only** command to make outbound BGP updates carry private AS numbers.

By default, a BGP update carries private AS numbers.

If a BGP update to be sent carries any public AS number, this command does not take effect. The private AS number ranges from 64512 to 65535.

Examples

In BGP-VPNv4 subaddress family view, configure the device to make BGP updates to be sent to peer group test carry no private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test public-as-only
```

peer reflect-client

Syntax

peer { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

Description

Use the **peer reflect-client** command to configure the local device to be a route reflector (RR) and set a peer or peer group as the client of the RR.

Use the **undo peer reflect-client** command to remove the configuration.

By default, no RR or RR client is configured.

Examples

In BGP-VPNv4 subaddress family view, configure the local device to be an RR and set peer group test as the client of the RR.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test reflect-client
```

In BGP-L2VPN address family view, configure the local device to be an RR and set peer group test as the client of the RR.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer test reflect-client
```

peer route-policy (BGP-VPNv4 subaddress family view)

Syntax

peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

ip-address: IP address of the peer.

route-policy-name: Name of the routing policy, a string of 1 to 19 characters.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description

Use the **peer route-policy** command to apply a routing policy to a peer or peer group.

Use the **undo peer route-policy** command to remove the application.

By default, no routing policy is applied to a peer or peer group.

Examples

In BGP-VPNv4 subaddress family view, apply routing policy test-policy to peer group test to filter the received routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test route-policy test-policy import
```

peer vpn-instance enable

Syntax

peer { *group-name* | *peer-address* } **vpn-instance** *vpn-instance-name* **enable**

undo peer { *group-name* | *peer-address* } **vpn-instance** *vpn-instance-name* **enable**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

peer-address: IP address of the peer.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

Description

Use the **peer vpn-instance enable** command to activate a nested VPN peer or peer group and enable the capability of exchanging BGP-VPNv4 routes with the peer or peer group.

Use the **undo peer vpn-instance enable** command to disable the capability of exchanging BGP-VPNv4 routes with a nested VPN peer or peer group.

By default, nested VPN peers/peer groups can exchange only IPv4 routes; they cannot exchange BGP-VPNv4 routes.

Note that:

- This configuration takes effect only after the nested VPN function is enabled.
- Before specifying a nested VPN peer or peer group, be sure to configure the corresponding CE peer or peer group using the **peer as-number** command in BGP-VPN instance view.
- Deleting the VPN instance to which a peer belongs will also delete the configuration of this command.

Examples

Activate a nested VPN peer group named **ebgp**.

```
<Sysname> system-view
[Sysname] bgp 10
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group ebgp external
```

```
[Sysname-bgp-vpn1] quit
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer ebgp vpn-instance vpn1 enable
```

peer vpn-instance group

Syntax

peer *peer-address* **vpn-instance** *vpn-instance-name* **group** *group-name*

undo peer *peer-address* **vpn-instance** *vpn-instance-name* **group** *group-name*

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

peer-address: IP address of the peer.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters..

Description

Use the **peer vpn-instance group** command to add a peer to a nested VPN peer group.

Use the **undo peer vpn-instance group** command to remove a peer from a nested VPN peer group.

By default, a peer is not in any nested peer group.

Note that:

- This configuration takes effect only after the nested VPN function is enabled.
- Deleting the VPN instance to which a peer belongs will also delete the configuration of this command.

Examples

Add peer 1.1.1.1 to the nested VPN peer group named **ebgp**.

```
<Sysname> system-view
[Sysname] bgp 10
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group ebgp external
[Sysname-bgp-vpn1] peer 1.1.1.1 as-number 600
[Sysname-bgp-vpn1] peer 1.1.1.1 group ebgp
[Sysname-bgp-vpn1] quit
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer ebgp vpn-instance vpn1 enable
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 vpn-instance vpn1 group ebgp
```

peer vpn-instance route-policy import

Syntax

peer { *group-name* | *peer-address* } **vpn-instance** *vpn-instance-name* **route-policy** *route-policy-name* **import**

undo peer { *group-name* | *peer-address* } **vpn-instance** *vpn-instance-name* **route-policy** *route-policy-name* **import**

View

BGP-VPNv4 subaddress family view

Default Level

2: System level

Parameters

group-name: Name of the peer group, a case-sensitive string of 1 to 47 characters.

peer-address: IP address of the peer, in dotted decimal notation.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

route-policy-name: Name of the routing policy to be applied, a case-sensitive string of 1 to 19 characters.

Description

Use the **peer vpn-instance route-policy import** command to specify the routing policy to be applied to VPNv4 routes received from a nested VPN peer or peer group.

Use the **undo peer vpn-instance route-policy import** command to restore the default.

By default, no routing policy is applied.

A routing policy for a peer and a routing policy for the peer group to which the peer belongs are of the same priority; the one configured last takes effect.

Note that:

- This configuration takes effect only after the nested VPN function is enabled.
- Deleting the VPN instance to which a peer belongs will also delete the configuration of this command.

Examples

Specify to apply routing policy **comtest** to VPNv4 routes received from peer group **ebgp**.

```
<Sysname> system-view
[Sysname] bgp 10
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer ebgp vpn-instance vpn1 route-policy comtest import
```

policy vpn-target

Syntax

policy vpn-target

undo policy vpn-target

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

None

Description

Use the **policy vpn-target** command to enable VPN target filtering for received VPNv4 routes.

Use the **undo policy vpn-target** command to disable the filtering, permitting all VPNv4 routes.

Only VPNv4 routes with export route target attributes matching the local import route target attributes are added into the routing table.

By default, the VPN target filtering function is enabled for received VPNv4 routes.

 **Note**

The command applies to inter-provider VPN option B schemes.

Examples

In BGP-VPNv4 subaddress family view, enable VPN target filtering for received VPNv4 routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] policy vpn-target
```

In BGP-L2VPN address family view, enable VPN target filtering for received VPNv4 routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] policy vpn-target
```

reflect between-clients

Syntax

reflect between-clients

undo reflect between-clients

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable the function.

By default, route reflection between clients is enabled.

If fully meshed interconnections exist between the clients, route reflection is not required. Otherwise, an RR is required for routes to be reflected from one client to every other client.

Examples

In BGP-VPNv4 subaddress family view, disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] undo reflect between-clients
```

In BGP-L2VPN address family view, disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] undo reflect between-clients
```

reflector culster-id

Syntax

reflector cluster-id { *cluster-id* | *ip-address* }

undo reflector cluster-id

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

cluster-id: Cluster ID of the route reflector (RR), in the range 1 to 4294967295.

ip-address: IP address of the peer, which is to be used as the cluster ID of the RR.

Description

Use the **reflector cluster-id** command to specify a cluster ID for an RR.

Use the **undo reflector cluster-id** command to remove the cluster ID.

By default, the cluster ID is the router ID of an RR in the cluster.

Generally, a cluster contains only one RR, in which case the router ID of the RR is used for identifying the cluster. Setting multiple RRs can improve the network reliability. When there is more than one RR in a cluster, use the **reflector cluster-id** command to configure the same cluster ID for all RRs in the cluster.

Examples

In BGP-VPNv4 subaddress family view, configure the local router as an RR of a cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] reflector cluster-id 50
```

In BGP-L2VPN address family view, configure the local router as an RR of a cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] reflector cluster-id 50
```

refresh bgp vpn-instance

Syntax

refresh bgp vpn-instance *vpn-instance-name* { *ip-address* | **all** | **external** | **group** *group-name* } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: Performs a soft reset of the BGP connection with a BGP peer identified by this IP address.

all: Performs a soft reset of all BGP VPN instance connections.

external: Performs a soft reset of EBGP sessions.

group *group-name*: Performs a soft reset of the connections with a BGP peer group identified by this name. The *group-name* argument is a string of 1 to 47 characters.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description

Use the **refresh bgp vpn-instance** command to perform a soft reset of BGP connections in a VPN instance.

Examples

Perform a soft reset of all BGP connections in VPN instance vpn1 in the inbound direction to make new configurations take effect.

```
<Sysname> refresh bgp vpn-instance vpn1 all import
```

refresh bgp vpnv4

Syntax

refresh bgp vpnv4 { *ip-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** }

View

User view

Default Level

1: Monitor level

Parameters

ip-address: Performs a soft reset of the BGP VPNv4 connection with a BGP peer identified by this IP address.

all: Performs a soft reset of all BGP VPNv4 connections.

external: Performs a soft reset of EBGP sessions.

group *group-name*: Performs a soft reset of the VPNv4 connections with a BGP peer group identified by this name.

internal: Performs a soft reset of IBGP sessions.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description

Use the **refresh bgp vpnv4** command to perform a soft reset of BGP VPNv4 connections.

Examples

Perform a soft reset of all BGP VPNv4 connections in the inbound direction to make new configurations take effect.

```
<Sysname> refresh bgp vpnv4 all import
```

reset bgp vpn-instance

Syntax

reset bgp vpn-instance *vpn-instance-name* { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* }

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

as-number: Resets BGP connections with the peers in an AS identified by this number. This argument is in the range 1 to 65535.

ip-address: Resets the connection with a BGP peer identified by this IP address.

group *group-name*: Resets the connections with a BGP peer group identified by this name. The *group-name* argument is a string of 1 to 47 characters.

all: Resets all BGP connections.

external: Resets EBGP sessions.

Description

Use the **reset bgp vpn-instance** command to reset the BGP connections of a VPN instance.

Examples

Reset all BGP connections of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 all
```

reset bgp vpn-instance dampening

Syntax

reset bgp vpn-instance *vpn-instance-name* **dampening** [*network-address* [*mask* | *mask-length*]]

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

dampening: Specifies route flap dampening information.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

Description

Use the **reset bgp vpn-instance dampening** command to clear the route flap dampening information of a VPN instance.

Examples

Clear the route flap dampening information of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 dampening
```

reset bgp vpn-instance flap-info

Syntax

reset bgp vpn-instance *vpn-instance-name ip-address* **flap-info**

reset bgp vpn-instance *vpn-instance-name* **flap-info** [*ip-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **regexp** *as-path-regexp*]

View

User view

Default Level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: IP address of the BGP peer.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

as-path-acl-number: Number of the AS_PATH list, in the range 1 to 256.

as-path-regexp: AS_PATH regular expression.

Description

Use the **reset bgp vpn-instance flap-info** command to clear the route flap history information about BGP peers of a VPN instance.

Examples

Clear route flap history information about BGP peer 2.2.2.2 of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 2.2.2.2 flap-info
```

reset bgp vpnv4

Syntax

reset bgp vpnv4 { *as-number* | *ip-address* | **all** | **external** | **internal** | **group** *group-name* }

View

User view

Default Level

1: Monitor level

Parameters

as-number: Resets VPNv4 connections with the peers in an AS identified by this number.

ip-address: Resets the VPNv4 connection with a BGP peer identified by this IP address.

group-name: Resets the VPNv4 connections with a BGP peer group identified by this name.

all: Resets all BGP VPNv4 connections.

external: Resets EBGP sessions of VPNv4 connections.

internal: Resets IBGP sessions of VPNv4 connections.

Description

Use the **reset bgp vpnv4** command to reset BGP VPNv4 connections.

Examples

Reset all BGP VPNv4 connections to make new configurations take effect.

```
<Sysname> reset bgp vpnv4 all
```

route-distinguisher (VPN instance view)

Syntax

route-distinguisher *route-distinguisher*

View

VPN instance view

Default Level

2: System level

Parameters

route-distinguisher: Route distinguisher (RD) for the VPN instance, a string of 3 to 21 characters in either of the following two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

Description

Use the **route-distinguisher** command to configure a route distinguisher (RD) for a VPN instance.

An RD is used to create the routing and FIB of a VPN. By prefixing an RD to an IPv4 prefix, you get a VPN IPv4 prefix unique globally.

Note

- No RD is configured by default; you must configure an RD for each VPN instance.
- A VPN instance takes effect only after you configure an RD for it.
- Once you configure an RD for a VPN, you cannot remove the association.
- You cannot change an RD directly; you can only delete the VPN instance, and then re-create the VPN instance and re-configure a new RD.

Examples

Configure the RD of VPN instance vpn1.

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

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

route-tag

Syntax

route-tag *tag-value*

undo route-tag

View

OSPF view

Default Level

2: System level

Parameters

tag-value: Tag for identifying injected VPN routes, in the range 0 to 4294967295.

Description

Use the **route-tag** command to configure the tag for identifying injected VPN routes.

Use the **undo route-tag** command to restore the default.

If the AS number is not greater than 65535, the first two octets of the default tag is always 0xD000 and the last two octets is the AS number of the local BGP. For example, if the local BGP AS number is 100, the default tag is 3489661028 in decimal. If the AS number is greater than 65535, the default tag is 0.

An OSPF instance-related VPN instance on a PE is usually configured with a VPN route tag, which must be included in Type 5/7 LSAs. PEs in the same AS are recommended to have the same route tag. The route tag is local significant and can be configured and take effect on only PEs receiving BGP routes and generating OSPF LSAs; it is not transferred in any BGP extended community attribute. Different OSPF processes can have the same route tag.

Tags configured with different commands have different priorities:

- A tag configured with the import-route command has the highest priority.
- A tag configured with the route-tag command has the second highest priority.
- A tag configured with the default tag command has the lowest priority.

A received Type 5 or Type 7 LSA is neglected in route calculation if its tag is the same as the local one.

Note

A configured route tag takes effect after you issue the **reset ospf** command.

Related commands: **import-route** in *OSPF Commands* of the *IP Routing Volume*.

Examples

Configure the route tag for OSPF process 100 as 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] route-tag 100
```

routing-table limit

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

View

VPN instance view

Default Level

2: System level

Parameters

number: Maximum number of routes for the VPN instance to support, in the range 1 to 128000..

warn-threshold: Threshold for warning. It is expressed in the maximum percentage of the number of routes for the VPN instance. It ranges from 1 to 100. When the specified threshold is reached, the system gives an alarm message but still allows new routes. If the number of routes received reaches the maximum supported, no more routes will be activated..

simply-alert: Specifies that when the maximum number of routes exceeds the threshold, the system still accepts routes and generates only a SYSLOG error message.

Description

Use the **routing-table limit** command to limit the maximum number of routes in a VPN instance, preventing too many routes from being accepted by a PE.

Use the **undo routing-table limit** command to cancel the configured limit.

Examples

Specify that VPN instance vpn1 can receive up to 1000 routes, and can receive new routes after the threshold is exceeded.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

rr-filter

Syntax

rr-filter *extended-community-list-number*

undo rr-filter

View

BGP-VPNv4 subaddress family view, BGP-L2VPN address family view

Default Level

2: System level

Parameters

extended-community-list-number: Number of the extended community list supported by the RR group, in the range 1 to 199.

Description

Use the **rr-filter** command to create an RR reflection policy.

Use the **undo rr-filter** command to disable the function.

Only IBGP routes whose route target extended community attributes satisfy the matching conditions are reflected. This provides a way to implement load balancing between RRs.

Examples

In BGP-VPNv4 subaddress family view, create an RR group and configure it to automatically filter the incoming VPNv4 route update packets based on the route target extended community attribute.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] rr-filter 10
```

In BGP-L2VPN address family view, create an RR group and configure it to automatically filter the incoming VPNv4 route update packets based on the route target extended community attribute.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] rr-filter 10
```

sham-link

Syntax

sham-link *source-ip-address destination-ip-address* [**cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retrans-interval* | **trans-delay** *delay* | **simple** [**cipher** | **plain**] *password1* | { **md5** | **hmac-md5** } *key-id* [**cipher** | **plain**] *password2*] *

undo sham-link *source-ip-address destination-ip-address* [**cost** | **dead** | **hello** | **retransmit** | **trans-delay** | **simple** | { **md5** | **hmac-md5** } *key-id*] *

View

OSPF area view

Default Level

2: System level

Parameters

source-ip-address: Source IP address for the sham link.

destination-ip-address: Destination IP address for the sham link.

cost: Cost for the sham link. It ranges from 1 to 65,535 and defaults to 1.

dead-interval: Dead Interval in seconds. It ranges from 1 to 32,768 and defaults to 40. It must be equal to the dead interval of the router on the other end of the virtual link and be at least four times the hello interval.

hello-interval: Interval at which the interface sends Hello packets. It ranges from 1 to 8,192 seconds and defaults to 10 seconds. It must be equal to the hello interval of the router on the other end of the virtual link.

retrans-interval: Interval at which the interface retransmits LSAs. It ranges from 1 to 8,192 seconds and defaults to 5 seconds.

delay: Delay interval before the interface sends an LSA. It ranges from 1 to 8,192 seconds and defaults to 1 second.

simple [**cipher** | **plain**] *password1*: Uses simple authentication. If you specify neither the **cipher** nor the **plain** keyword, the *password1* argument is a string of 1 to 8 characters. For the plain mode, the *password1* argument is a string of 1 to 8 characters. For the cipher mode, the *password1* argument can be either a string of 1 to 8 characters in plain text, or a string of 24 characters in cipher text.

md5: Uses MD5 algorithm for authentication.

hmac-md5: Uses HMAC-MD5 algorithm for authentication.

key-id: Authentication key ID of the interface, in the range 1 to 255. It must be the same as that of the peer.

cipher: Uses cipher text.

plain: Uses plain text.

password2: Password string, case-sensitive. If you specify neither the **cipher** nor the **plain** keyword, it is a string of 1 to 16 characters in plain text or a string of 24 characters in cipher text. For the plain mode, it is a string of 1 to 16 characters. For the cipher mode, it can be either a string of 1 to 16 characters in plain text, or a string of 24 characters in cipher text.

Description

Use the **sham link** command to configure a sham link.

Use the **undo sham link** command with no optional keyword to remove a sham link.

Use the **undo sham link** command with optional keywords to restore the defaults of the parameters for a sham link.

If two PEs belong to the same AS and a backdoor link is present, a sham link can be established between them.

For plain text authentication, the default authentication key type is plain. For authentication using MD5 algorithm or HMAC-MD5 algorithm, the default authentication key type is cipher.

Examples

Create a sham link with the source address of 1.1.1.1 and the destination address of 2.2.2.2.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] sham-link 1.1.1.1 2.2.2.2
```

tnl-policy (VPN instance view)

Syntax

tnl-policy *tunnel-policy-name*

undo tnl-policy

View

VPN instance view

Default Level

2: System level

Parameters

tunnel-policy-name: Name of the tunneling policy for the VPN instance, a string of 1 to 19 characters.

Description

Use the **tnl-policy** command to associate the current VPN instance with a tunneling policy.

Use the **undo tnl-policy** command to remove the association.

When selecting tunnels from the VPN tunnel management module, an application can use the tunneling policy as the criterion. With no tunneling policy associated with a VPN instance, the default tunneling policy is used.

Related commands: **tunnel select-seq load-balance-number**.

Examples

Associate VPN instance vpn2 with tunneling policy po1.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1] tunnel select-seq lsp load-balance-number 1
[Sysname-tunnel-policy-po1] quit
[Sysname] ip vpn-instance vpn2
[Sysname-vpn-instance-vpn2] route-distinguisher 22:33
[Sysname-vpn-instance-vpn2] tnl-policy po1
```

tunnel-policy

Syntax

tunnel-policy *tunnel-policy-name*

undo tunnel-policy *tunnel-policy-name*

View

System view

Default Level

2: System level

Parameters

tunnel-policy-name: Name for the tunneling policy, a string of 1 to 19 characters.

Description

Use the **tunnel-policy** command to establish a tunneling policy and enter tunneling policy view.

Use the **undo tunnel-policy** command to delete a tunneling policy.

Related commands: **tunnel select-seq load-balance-number**.

Examples

Establish a tunneling policy named po1 and enter tunneling policy view.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1]
```

tunnel select-seq load-balance-number

Syntax

tunnel select-seq { **cr-lsp** | **lsp** } * **load-balance-number** *number*

undo tunnel select-seq

View

Tunneling policy view

Default Level

2: System level

Parameters

cr-lsp: Specifies CR-LSP tunnels.

lsp: Specifies LSP tunnels.

number: Number of tunnels for load balancing, in the range 1 to 4.

Description

Use the **tunnel select-seq load-balance-number** command to configure the preference order for tunnel selection and the number of tunnels for load balancing.

Use the **undo tunnel select-seq** command to restore the default.

Note

The S7900E series switches do not support CR-LSP tunnels. You can configure load balancing for only LSP tunnels.

By default, one LSP tunnel can be used. That is, only LSP tunnels can be used and the number of tunnels for load balancing is 1.

Examples

Define a tunneling policy, specifying that only GRE tunnels can be used and the number of tunnels for load balancing be 2.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1] tunnel select-seq gre load-balance-number 2
```

vpn-target (VPN instance view)

Syntax

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | { *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

View

VPN instance view

Default Level

2: System level

Parameters

vpn-target&<1-8>: Adds the VPN target extended community attribute to the import or export VPN target extended community list and specify the VPN target in the format nn:nn or IP-address:nn. &<1-8> means that you can specify this argument for up to 8 times.

A VPN target attribute can be of 3 to 21 characters and in either of these two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

both: Specifies both the export routing information to the destination VPN extended community and the import routing information from the destination VPN extended community. This is the default.

export-extcommunity: Specifies the export routing information to the destination VPN extended community.

import-extcommunity: Specifies the import routing information from the destination VPN extended community.

all: Specifies all export routing information to the destination VPN extended community and import routing information from the destination VPN extended community.

Description

Use the **vpn-target** command to associate the current VPN instance with one or more VPN targets.

Use the **undo vpn-target** command to remove the association of the current VPN instance with VPN targets.

VPN target has no default. You must configure it when creating a VPN instance.

Examples

Associate the current VPN instance with VPN targets.

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

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
 EVT Assignment result:
 VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
 IVT Assignment result:
 VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
 IVT Assignment result:
 VPN-Target assignment is successful
 EVT Assignment result:
 VPN-Target assignment is successful
```

QoS Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The QoS Volume is organized as follows:

Features	Description
QoS	Quality of Service (QoS) reflects the ability to meet customer needs. This documentation mainly describes the commands for： • traffic classification configuration • traffic policing configuration • traffic shaping configuration • line rate configuration • QoS policy configuration • congestion management configuration • congestion avoidance configuration • priority mapping configuration • QoS in an EPON system

Table of Contents

1 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: GigabitEthernet2/0/1
Rule(s): If-match queue 2
 CIR 640 (kbps), CBS 40960 (byte)
```

Table 1-1 Description on the fields of the **display qos gts** command

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. For GigabitEthernet ports, CIR ranges from 64 to 1048576; for ten-GigabitEthernet ports, CIR ranges from 64 to 10485760.

cbs *committed-burst-size*: Specifies the CBS (in bytes), which ranges from 4096 to 268435456 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 268435456. 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 2/0/1 to limit the outgoing traffic rate of queue 2 to 640 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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: GigabitEthernet2/0/10
Direction: Outbound
 CIR 64000 (kbps),  CBS 4000000 (byte)
```

Table 1-2 Description on the fields of the **display qos lr** command

Field	Description
Interface	Port name, composed of port type and port number
Direction	Specify the direction of limited rate as outbound
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:

- Fast Ethernet port: 64 to 100000
- 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 2/0/1 within 640 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos lr outbound cir 640
```

2 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 2-1 Description on the fields of the **display traffic classifier user-defined** command

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 2-2 describes the available forms of this argument.

Table 2-2 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 in the range 2000 to 4999. 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 in the range 2000 to 3999. 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. You can provide up to eight space-separated CoS values for this argument. CoS is in the range 0 to 7.
dscp *dscp-list*	Specifies to match packets by DSCP precedence. The *dscp-list* argument is a list of DSCP values. You can provide up to eight space-separated DSCP values for this argument. DSCP is in the range 0 to 63.
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. You can provide up to eight space-separated IP precedence values for this argument. IP precedence is in the range 0 to 7.
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. You can provide up to eight space-separated CoS values for this argument. CoS is in the range 0 to 7.
source-mac *mac-address*	Specifies to match the packets with a specified source MAC address.

Field	Description
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**.
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**.

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 VLAN 1024 of the customer network.

```
<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 VLAN 1000 of the service provider network.

```
<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 10000000 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 10000000 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 2-3 Description on the fields of the **display traffic behavior user-defined** command

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
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
```

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.

Note that when the action of mirroring traffic is applied in the outbound direction of an SC LPU, any other action cannot be configured in the same traffic behavior. Otherwise, the corresponding QoS policy cannot be applied successfully.

Examples

Configure traffic behavior 1 and define the action of mirroring traffic to GigabitEthernet2/0/2 in the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface GigabitEthernet 2/0/2
```

nest

Syntax

nest top-most vlan-id *vlan-id*

undo nest

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:

- If the **nest** action will be applied to the inbound direction of a port or port group on an EA LPU, the classification rule must be configured with the **if-match customer-vlan-id** command, and the other actions except **remark dot1p** cannot be configured in the traffic behavior. Additionally, you must enable basic QinQ on the port or port group before applying the QoS policy.
- If the **nest** action will be applied to the inbound direction of a port or port group on an SA or SC LPU, you must enable basic QinQ on the port or port group first.
- 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
```

redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** { *ipv4-add* [*ipv4-add*] | *ipv6-add* [*interface-type interface-number*] [*ipv6-add* [*interface-type interface-number*]] } }

undo redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** }

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.

next-hop: Specifies the next hop to redirect the traffic to.

ipv4-add: IPv4 address of the next hop.

ipv6-add: IPv6 address of the next hop. The *interface-type interface-number* argument is a VLAN interface number. If the IPv6 address is a link-local address, you must specify a VLAN interface for the IPv6 address of the next hop; if the IPv6 address is not a link-local address, you need not specify a VLAN interface for the IPv6 address of the next hop.

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 GigabitEthernet2/0/1 port.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface GigabitEthernet 2/0/1
```

remark customer-vlan-id

Syntax

remark customer-vlan-id *vlan-id-value*

undo remark customer-vlan-id

View

Traffic behavior view

Default Level

2: System Level

Parameters

vlan-id-value: VLAN ID to be set for packets, in the range of 1 to 4094.

Description

Use the **remark customer-vlan-id** command to configure the action of setting the customer network VLAN ID for a traffic behavior.

Use the **undo remark customer-vlan-id** command to remove the action of setting the customer network VLAN ID.

Note that the action of setting the customer network VLAN ID cannot be applied to a VLAN or applied globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action of setting the customer network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark customer-vlan-id 2
```

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 2-4.

Table 2-4 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

Keyword	DSCP value (binary)	DSCP value (decimal)
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
```

remark service-vlan-id

Syntax

remark service-vlan-id *vlan-id-value*

undo remark service-vlan-id

View

Traffic behavior view

Default Level

2: System Level

Parameters

vlan-id-value: VLAN ID to be set for packets, in the range of 1 to 4094.

Description

Use the **remark service-vlan-id** command to configure the action of setting the service provider network VLAN ID for a traffic behavior.

Use the **undo remark service-vlan-id** command to remove the action of setting the service provider network VLAN ID.

- Note that: If the **remark service-vlan-id** action will be applied to the inbound direction of a port or port group on an EA LPU, the classification rule must be configured with the **if-match customer-vlan-id** command, and the other actions except **remark dot1p** cannot be configured in the traffic behavior.
- If the **remark service-vlan-id** action will be applied to the outbound direction of a port or port group on an SC LPU, any other actions except **filer** and **remark dot1p** cannot be configured in the traffic behavior.
- The **remark service-vlan-id** action cannot be applied to a VLAN or applied globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action of setting the service provider network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark service-vlan-id 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.

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* [**mode do1q-tag-manipulation**]

undo classifier *classifier-name*

View

Policy view

Default Level

2: System Level

Parameters

classifier-name: Name of an existing class.

behavior–name: Name of an existing traffic behavior.

mode dot1q-tag-manipulation: Specifies that the association relationship between the class and the traffic behavior is used for the VLAN mapping function.

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**.

Note

In a QoS policy with multiple class-to-traffic-behavior associations, if the action of creating an outer VLAN tag, the action of setting customer network VLAN ID, or the action of setting service provider network VLAN ID is configured in a traffic behavior, we recommend you not to configure any other action in this traffic behavior. Otherwise, the QoS policy may not function as expected after it is applied.

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. If it is not provided, the configuration of all the user defined policies is displayed.

classifier-name: Name of a class in the policy. If it is not provided, all the classes in the policy are specified.

Description

Use the **display qos policy** command to display the configuration of a specified 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 2-5 Description on the fields of the **display qos policy** command

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 { **inbound** | **outbound** } [**slot** *slot-id*]

View

Any view

Default Level

1: Monitor level

Parameters

inbound: Displays the QoS policy applied globally in the inbound direction of all ports.

outbound: Displays the QoS policy applied globally in the outbound direction of all ports.

slot *slot-number*: Displays the global QoS policy applied on a board. If the *slot-number* argument is not specified, the global QoS policy applied on the main control board are displayed.

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 2-6 Description on the fields of the **display qos policy global** command

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
Behavior	Traffic behavior name

display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound 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 on GigabitEthernet2/0/1 port.

```
<Sysname> display qos policy interface GigabitEthernet 2/0/1

  Interface: GigabitEthernet2/0/1
```

```
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 2-7 Description on the fields of the **display qos policy interface** command

Field	Description
Interface	Port name, comprising of port type and port number
Direction	Direction of the port where the policy is applied
Policy	Name of the policy applied to the port
Classifier	Name of the class in the policy and its configuration **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 of the behavior in the policy and its configuration

display qos vlan-policy

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-id*]

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.

vlan *vlan-id*: Specifies to display the information about the VLAN policy applied to the specified VLAN.

slot-id: Specifies to display the information about the VLAN policies applied to VLANs on the board seated in the specific slot. If the *slot-id* argument is not specified, this command displays the information about the VLAN policies applied to the SRPU.

Description

Use the **display qos vlan-policy** command to display the information about VLAN policies.

If the *vlan-id* argument is not specified, the information about all the VLAN policies will be displayed.

Examples

Display the information about the VLAN policy named test.

```
<Sysname> display qos vlan-policy name test
  Policy test
    Vlan 300: inbound
```

Table 2-8 Description on the fields of the **display qos vlan-policy** command

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 2-9 Description on the fields of the **display qos vlan-policy** command

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
Behavior	Name of the behavior in the policy and its configuration

qos apply policy

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy { **inbound** | **outbound** }

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

policy-name: Specifies the policy name.

Description

Use the **qos apply policy** command to apply a 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.

Note that, when you apply a policy by using the **qos apply policy** command, whether or not the **inbound**/**outbound** keyword can take effect depends on the actions defined in the traffic behavior and LPU types, as described in Table 2-10.

Table 2-10 The support for the inbound direction and the outbound direction

LPU type / Action	SC LPU		SA LPU		EA LPU	
	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
Traffic accounting	Supported	Supported	Supported	Not supported	Supported	Not supported
TP	Supported	Supported	Supported	Not supported	Supported	Not supported
Traffic filtering	Supported	Supported	Supported	Not supported	Supported	Not supported
Traffic mirroring	Supported	Supported	Supported	Not supported	Supported	Not supported
Configuring the outer VLAN tag	Supported	Not supported	Supported	Not supported	Supported	Not supported
Traffic redirecting	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the customer network VLAN ID for packets	Not supported	Supported	Not supported	Not supported	Not supported	Not supported

LPU type / Action	SC LPU		SA LPU		EA LPU	
	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
Remarking the 802.1p precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the drop precedence for packets	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the DSCP precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the IP precedence for packets	Supported	Supported	Supported	Not supported	Supported	Not supported
Remarking the local precedence for packets	Supported	Not supported	Supported	Not supported	Supported	Not supported
Remarking the service provider network VLAN ID for packets	Supported	Supported	Supported	Not supported	Supported	Not supported

Note

SC LPUs include LSQ1GP24SC LPUs and so on, SA LPUs include LSQ1FP48SA LPUs and so on, EA LPUs include LSQ1GP12EA LPUs and so on. For the detailed information about LPU types, refer to the installation manual.

Caution

You can apply a QoS policy in the outbound direction of a basic QinQ-enabled port on an SA LPU or EA LPU to implement one-to-one VLAN mapping. In this policy, only one matching rule, **if-match service-vlan-id**, can be defined, and the action can only be **remark customer-vlan-id** or **remark customer-vlan-id** together with **remark dot1p**.

Examples

Apply the policy named test in the inbound direction of GigabitEthernet2/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos apply policy test inbound
```

qos apply policy global

Syntax

qos apply policy *policy-name* **global** { **inbound | outbound** }

undo qos apply policy global { **inbound | outbound** }

View

System view

Default Level

2: System Level

Parameters

policy-name: Policy name.

inbound: Applies the QoS policy to the incoming packets on all ports.

outbound: Applies the QoS policy to the outgoing 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 or outbound 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.

Note that, when you apply a QoS policy with the **qos apply policy global** command, support for the **inbound**/**outbound** keyword depends on the actions defined in the traffic behavior and LPU types, as described in Table 2-10.

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.

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** | **outbound** }

undo qos vlan-policy vlan *vlan-id-list* { **inbound** | **outbound** }

View

System view

Default Level

2: System Level

Parameters

policy-name: 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.

outbound: Specifies to apply the VLAN policy in the outbound 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 that, when you apply a QoS policy with the **qos vlan-policy** command, support for the **inbound**/**outbound** keyword varies with the actions defined in the traffic behavior and the type of the LPU to which the ports in the VLAN belong, as described in Table 2-10.

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** | **outbound** }

View

User view

Default Level

1: Monitor level

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

Description

Use the **reset qos vlan-policy** command to clear the statistics of a global QoS policy.

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*]

View

User view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range 1 to 4,094.

Description

Use the **reset qos vlan-policy** command to clear the statistics information about VLAN policies.

Examples

Clear the statistics information about the VLAN policy applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

3 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 2/0/1.

```
<Sysname> display qos sp interface GigabitEthernet 2/0/1
Interface: GigabitEthernet2/0/1
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 3/0/1 on an EA LPU.

```
< Sysname > display qos wfq interface e 3/0/1
Interface: Ethernet3/0/1
 Output queue: Hardware weighted fair queue
Queue ID         Weight          Min-Bandwidth
-----------------------------------------------
0                1               64
1                1               64
2                1               64
3                1               64
4                1               64
5                1               64
6                1               64
7                1               64
```

Display the configuration of the WFQ queues on port GigabitEthernet 2/0/1 on a non-EA LPU.

```
<Sysname> display qos wfq interface GigabitEthernet 2/0/1
Interface: GigabitEthernet2/0/1
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 3-1 Description on the fields of the **display qos wfq interface** command

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 2/0/1.

```
<Sysname> display qos wrr interface GigabitEthernet 2/0/1
Interface: GigabitEthernet2/0/1
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 3-2 Description on the fields of the **display qos wrr interface** command

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 2/0/1.

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

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet 2/0/1] qos wfq
[Sysname-GigabitEthernet 2/0/1] 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, the switch adopts the SP queue-scheduling algorithm.

Related commands: **display qos sp interface**.

Examples

Configure SP queuing on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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, the switch adopts the SP queue-scheduling algorithm.

Related commands: **display qos wrr interface**.

Examples

Enable WFQ on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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. The range for the scheduling weight depends on the LPU type of your S7900E series switch:

- For EA LPUs, the scheduling weight of each queue is 1, that is, all queues share the allocable bandwidth (allocable bandwidth = total bandwidth – the sum of the minimum guaranteed bandwidth for each queue).
- For non-EA LPUs, the scheduling weight 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 2/0/1 on a non-EA LPU and assign weight values 1, 2, 4, 6, 8, 10, 12, and 14 to queues 0 through 7.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos wfq
[Sysname-GigabitEthernet2/0/1] qos wfq 0 weight 1
[Sysname-GigabitEthernet2/0/1] qos wfq 1 weight 200
[Sysname-GigabitEthernet2/0/1] qos wfq 2 weight 4
[Sysname-GigabitEthernet2/0/1] qos wfq 3 weight 6
[Sysname-GigabitEthernet2/0/1] qos wfq 4 weight 8
[Sysname-GigabitEthernet2/0/1] qos wfq 5 weight 10
[Sysname-GigabitEthernet2/0/1] qos wfq 6 weight 12
[Sysname-GigabitEthernet2/0/1] 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, the switch adopts the SP queue-scheduling algorithm.

On a port or port group with WRR enabled, the weight values of queues 0 through 7 are 1, 2, 3, 4, 5, 6, 7, and 8 respectively.

Related commands: **display qos wrr interface**.

Examples

Enable WRR on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos wrr
```

qos wrr weight

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, the switch adopts the SP queue-scheduling algorithm.

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 2/0/1 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 2/0/1
[Sysname-GigabitEthernet2/0/1] qos wrr
[Sysname-GigabitEthernet2/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet2/0/1] qos wrr 1 group sp
[Sysname-GigabitEthernet2/0/1] qos wrr 2 group sp
[Sysname-GigabitEthernet2/0/1] qos wrr 3 group sp
[Sysname-GigabitEthernet2/0/1] qos wrr 4 group 1 weight 2
[Sysname-GigabitEthernet2/0/1] qos wrr 5 group 1 weight 4
[Sysname-GigabitEthernet2/0/1] qos wrr 6 group 1 weight 6
[Sysname-GigabitEthernet2/0/1] qos wrr 7 group 1 weight 8
```

4 Congestion Avoidance Configuration Commands

Congestion Avoidance Configuration Commands

display qos wred interface

Syntax

display qos wred 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 wred interface** command to display the WRED configuration of a port.

If no port number is specified, the command displays the WRED configurations of all ports.

Related commands: **qos wred apply**.

Examples

Display the WRED configuration of GigabitEthernet 2/0/1.

```
<Sysname> display qos wred interface GigabitEthernet 2/0/1
Interface: GigabitEthernet2/0/1
 Current WRED configuration:
 Applied WRED table name: queue-table1
```

display qos wred table

Syntax

display qos wred table [*table-name*]

View

Any view

Default Level

1: Monitor level

Parameters

table-name: Name of the WRED table to be displayed.

Description

Use the **display qos wred table** command to display the WRED table configuration information.

If no WRED table name is specified, the configuration of all the WRED tables is displayed.

Related commands: **queue**.

Examples

Display the configuration of WRED table queue-table1.

```
<Sysname> display qos wred table queue-table1

Table Name: queue-table1
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob
------------------------------------------------------------------------
 0    10    NA    10    10    NA    10    10    NA    10
 1    10    NA    10    10    NA    10    10    NA    10
 2    10    NA    10    10    NA    10    10    NA    10
 3    10    NA    10    10    NA    10    10    NA    10
 4    10    NA    10    10    NA    10    10    NA    10
 5    10    NA    10    10    NA    10    10    NA    10
 6    10    NA    10    10    NA    10    10    NA    10
 7    10    NA    10    10    NA    10    10    NA    10
```

Table 4-1 display qos wred table command output description

Field	Description
Table name	Name of a WRED table
Table type	Type of a WRED table
Queue ID	ID of the queue
gmin	Lower threshold configured for green packets, whose drop precedence is 0
gmax	Upper threshold configured for green packets, whose drop precedence is 0
gprob	Drop probability slope configured for green packets, whose drop precedence is 0
ymin	Lower threshold configured for yellow packets, whose drop precedence is 1
ymax	Upper threshold configured for yellow packets, whose drop precedence is 1
yprob	Drop probability slope configured for yellow packets, whose drop precedence is 1
rmin	Lower threshold configured for red packets, whose drop precedence is 2
rmax	Upper threshold configured for red packets, whose drop precedence is 2
rprob	Drop probability slope configured for red packets, whose drop precedence is 2

qos wred apply

Syntax

qos wred apply *table-name*

undo qos wred apply

View

Interface view, port group view

Default Level

2: System Level

Parameters

table-name: Name of a global WRED table.

Description

Use the **qos wred apply** command to apply a WRED table to the current port or port group.

Use the **undo qos wred apply** command to cancel the application.

By default, no WRED table is applied to any port or port group.

Related commands: **display qos wred interface**.

Examples

Apply the WRED table **queue-table1** to the GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos wred apply queue-table1
```

qos wred queue table

Syntax

qos wred queue table *table-name*

undo qos wred table *table-name*

View

System view

Default Level

2: System Level

Parameters

table *table-name*: Specifies a name for the table, a string of 1 to 32 characters..

Description

Use the **qos wred queue table** command to create a WRED table and enter WRED table view.

Use the **undo qos wred table** command to remove a WRED table.

By default, no WRED table is created.

A WRED table in use cannot be removed.

Related commands: **queue**.

Examples

Create a WRED table named **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

queue

Syntax

queue *queue-id* [**drop-level** *drop-level*] **low-limit** *low-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-id* | **all** }

View

WRED table view

Default Level

2: System Level

Parameters

queue-id: ID of the queue, in the range of 0 to 7.

drop-level *drop-level*: Specifies a drop level, in the range of 0 to 2. If this argument is not specified, the subsequent configuration takes effect on the packets in the queue regardless of the drop level.

low-limit *low-limit*: Specifies a lower threshold. When the queue length exceeds the lower threshold, WRED begins to drop packets. The *low-limit* argument ranges from 0 to 100 and defaults to 10.

discard-probability *discard-prob*: Specifies the *discard-prob* argument, which ranges from 0 to 90 and defaults to 10. Each drop level is configured with an independent drop probability. The meaning of **discard-probability** *discard-prob* depends on the type of the LPU where the WRED table-applied port resides, as shown in Table 4-2.

Table 4-2 Description on **discard-probability** *discard-prob*

LPU type	Description on discard-probability *discard-prob*
EA	In a coordinate graph with the queue length percentage as the abscissa and drop probability as the ordinate, *discard-prob* specifies the degree of the included angle between the abscissa and the straight line starting at (low-limit, 0) and ending at (100%, max-drop-probability). The degree of the included angel ranges from 0 to 90. • When the queue length is fixed, the bigger the argument, the bigger the drop-probability. • When the argument is fixed, the bigger the queue length, the bigger the drop-probability.

LPU type	Description on discard-probability *discard-prob*
SC	Reciprocal of the drop probability. The argument corresponds to the drop probability as follows: • 0 corresponds to 100% • 1 through 8 corresponds to 1/8 • 9 through 16 corresponds to 1/16 • 17 through 32 corresponds to 1/32 • 33 through 64 corresponds to 1/64 • 65 through 90 corresponds to 1/128

Description

Use the **queue** command to configure the drop-related parameters for a specified queue in the WRED table.

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

By default, the lower threshold is 10 and the *discard-prob* argument is 10 for all the drop levels in the WRED table.

Related commands: **qos wred queue table**.

Examples

Modify drop parameters for queue 1 in the WRED table **queue-table1**: set the lower threshold to 10 and the degree of the included angle between the drop probability and queue length percentage to 30 for packets with drop level 1 in queue 1 (assuming the WRED table **queue-table1** is applied to a port on an EA LPU).

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 discard-probability 30
```

5 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 5-1 Description on the fields of the **display qos map-table** command

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

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.

export-value: Output parameter in the mapping table.

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
```

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]
```

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 GigabitEthernet2/0/1 port to 2.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 GigabitEthernet2/0/1 port.

```
<Sysname> display qos trust interface GigabitEthernet 2/0/1
Interface: GigabitEthernet2/0/1
Port priority information
Port priority :0
Port priority trust type : dscp
```

Table 5-2 Description on the fields of the **display qos trust interface** command

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

qos trust

Syntax

qos trust 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.

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 802.1p precedence of the received packets is trusted.

Examples

Specify to trust the DSCP precedence carried in packets on GigabitEthernet 2/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos trust dscp
```

6 QoS Configuration Commands in an EPON System

QoS Configuration Commands at the OLT Side

bandwidth downstream

Syntax

bandwidth downstream { **max-bandwidth** *value* | **max-burstsize** *value* } *

undo bandwidth downstream { **max-bandwidth** | **max-burstsize** } *

View

ONU port view

Default Level

2: System level

Parameters

max-bandwidth *value*: Specifies the maximum bandwidth in kbps. The *value* argument ranges from 0 to 999994. The system default is 999994 kbps.

max-burstsize *value*: Specifies the maximum burst buffer size in bytes. The *value* argument ranges from 0 to 8388480. The system default is 8388480 bytes.

Description

Use the **bandwidth downstream** command to configure the downlink bandwidth limit.

Use the **undo bandwidth downstream** command to restore the default.

Related commands: **bandwidth downstream policy enable**.

Note

- This command takes effect only when the downlink bandwidth allocation policy is enabled.
- The configured downlink bandwidth limit takes effect only on known unicasts, but not on unknown unicasts, multicasts, or broadcasts.

Examples

Set the downstream bandwidth limit to 800000 kbps and maximum burst size to 8000000 bytes on ONU 2/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] bandwidth downstream max-bandwidth 800000 max-burstsize 8000000
```

bandwidth downstream high-priority enable

Syntax

bandwidth downstream high-priority enable

undo bandwidth downstream high-priority enable

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **bandwidth downstream high-priority enable** command to reserve high-priority buffer for the ONU corresponding to the current port.

Use the **undo bandwidth downstream high-priority enable** command to restore the default.

By default, no high-priority packet buffer is reserved for any ONU.

Related commands: **bandwidth downstream priority-queue**.

Note

The high-priority packet buffer configuration takes effect only when the downlink bandwidth allocation policy is enabled.

Examples

Enable the high-priority packet buffer for the ONU corresponding to ONU 2/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] bandwidth downstream high-priority enable
```

bandwidth downstream policy enable

Syntax

bandwidth downstream policy enable

undo bandwidth downstream policy enable

View

ONU port view

Default Level

2: System level

Parameters

None

Description

Use the **bandwidth downstream** command to enable the downlink bandwidth allocation policy for the ONU port.

Use the **undo bandwidth downstream** command to restore the default.

By default, the downlink bandwidth allocation policy is disabled.

Related commands: **bandwidth downstream**.

Note

The downlink bandwidth limit configuration commands take effect only when the downlink bandwidth allocation policy is enabled.

Examples

Enable the downlink bandwidth allocation policy for ONU 2/0/1:1.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] bandwidth downstream policy enable
```

bandwidth downstream priority-queue

Syntax

bandwidth downstream priority-queue *priority* **high-priority-reserved** *value*

undo bandwidth downstream priority-queue high-priority-reserved

View

OLT port view

Default Level

2: System level

Parameters

priority: Queue priority, in the range 0 to 7.

value: Buffer size reserved for packets of high-priority queues, in bytes. It is in the range 0 to 131070 and defaults to 0.

Description

Use the **bandwidth downstream priority-queue** command to configure thresholds for high-priority queues and reserve user-defined buffer sizes for high-priority queues based on the thresholds.

Use the **undo bandwidth downstream priority-queue high-priority-reserved** command to cancel the configuration.

By default, no priority threshold or buffer size is set for high-priority packet buffer.

The downlink packets on an OLT port are considered as high-priority only if their priority is greater than or equal to the *priority* value.

This command just configures buffer parameters. To make these parameters take effect, use the **bandwidth downstream high-priority enable** command to enable high-priority packet buffer for the specified ONU.

Examples

Reserve 100 bytes of buffer for the packets whose priorities are greater than or equal to 3.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] bandwidth downstream priority-queue 3 high-priority-reserved 100
```

priority-queue-mapping

Syntax

priority-queue-mapping { **downstream** | **upstream**} { *value* } *&<1-8>*

undo priority-queue-mapping { **downstream** | **upstream**}

View

OLT port view

Default Level

2: System level

Parameters

downstream: Downlink packets.

upstream: Uplink packets.

value : Local precedence, in the range 0 to 7.

&<1-8>: Indicates that you can specify up to eight priority queue values.

Description

Use the **priority-queue-mapping** command to configure the mapping between the CoS precedence and local precedence of uplink and downlink packets on the OLT port.

Use the **undo priority-queue-mapping** command to restore the default mapping between CoS precedence and local precedence of uplink and downlink packets on the OLT port.

The default mapping between CoS precedence and local precedence on an OLT port is as shown in Table 6-1.

Table 6-1 Default mapping between the CoS precedence and local precedence of the packets on an OLT port

CoS precedence	Local precedence
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Examples

Configure the mapping between the CoS precedence and local precedence of downlink packets on the OLT port.

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] priority-queue-mapping downstream 1 1 2 3 4 5 6 7
```

Table 6-2 shows the mapping between CoS precedence and local precedence of downlink packets on the OLT port after the configuration is compete.

Table 6-2 Mapping between CoS precedence and local precedence

CoS precedence	Local precedence
0	1
1	1
2	2
3	3
4	4
5	5
6	6
7	7

QoS Configuration Commands at the ONU Side

qos cos-local-precedence-map

Syntax

qos cos-local-precedence-map *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*

undo qos cos-local-precedence-map

View

ONU port view

Default Level

2: System level

Parameters

cos0-map-local-prec: Local precedence to which CoS 0 is to be mapped, in the range of 0 to 3.

cos1-map-local-prec: Local precedence to which CoS 1 is to be mapped, in the range of 0 to 3.

cos2-map-local-prec: Local precedence to which CoS 2 is to be mapped, in the range of 0 to 3.

cos3-map-local-prec: Local precedence to which CoS 3 is to be mapped, in the range of 0 to 3.

cos4-map-local-prec: Local precedence to which CoS 4 is to be mapped, in the range of 0 to 3.

cos5-map-local-prec: Local precedence to which CoS 5 is to be mapped, in the range of 0 to 3.

cos6-map-local-prec: Local precedence to which CoS 6 is to be mapped, in the range of 0 to 3.

cos7-map-local-prec: Local precedence to which CoS 7 is to be mapped, in the range of 0 to 3.

Description

Use the **qos cos-local-precedence-map** command to configure the mappings between CoS precedence values to local precedence values on an ONU port.

Use the **undo qos cos-local-precedence-map** command to restore the mappings between CoS precedence values to local precedence values on an ONU port to defaults.

Table 6-3 shows the default CoS precedence values and the corresponding local precedence queues of the packets on an ONU port.

Caution

This command takes effect on the downlink data stream only.

Table 6-3 Default mapping between CoS precedence and local precedence

CoS precedence	Local precedence
0	0
1	0
2	1
3	1
4	2
5	2
6	3

CoS precedence	Local precedence
7	3

Examples

Configure the CoS precedence-to-local precedence mapping of the packets on the ONU port.

```
<Sysname> system-view
[Sysname] interface onu2/0/1:1
[Sysname-Onu2/0/1:1] qos cos-local-precedence-map 0 1 1 0 2 2 3 3
```

Table 6-4 shows the CoS precedence-to-local precedence mapping after the configuration is compete.

Table 6-4 CoS precedence-to-local precedence mapping

CoS precedence	Local precedence
0	0
1	1
2	1
3	0
4	2
5	2
6	3
7	3

uni classification-marking

Syntax

uni *uni-number* **classification-marking index** *index* **queue** *qid* **priority** *priority* { *selector operator matched-value* } *&<1-4>*

undo uni *uni-number* **classification-marking index** *index*

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

index: UNI index number, in the range 1 to 8. The match rule configured on the UNI port with the smallest index number is used first.

qid: Queue ID, in the range 0 to 7.

priority: Mapping priority, in the range 0 to 7.

selector: Match field.. Table 6-5 lists possible *selector* values.

operator: Match rule. Table 6-6 lists possible *operator* values.

matched-value: Match field value.

&<1-4>: Indicates that you can specify up to four values for the *selector*, *operator*, and *matched-value* arguments respectively.

Table 6-5 Selector values

Selector	Description
always-match	Perform a match on physical ports for traffic classification
dst-ip	Perform a match on the destination IP addresses of the packets
dst-mac	Perform a match on the destination MAC addresses of the packets
dst-port	Perform a match on the port numbers of the packets
eth-pri	Perform a match on the CoS precedence of the packets
eth-type	Perform a match on the Ethernet frame types of the packets
ip-precedence	Perform a match on the IP precedence of the packets
ip-tos-dscp	Perform a match on the ToS precedence or DSCP precedence of the packets
ip-type	Perform a match on the IP protocol types of the packets
never-match	Performs no traffic classification for the traffic received by the specified UNI port
src-ip	Perform a match on the source IP addresses of the packets
src-mac	Perform a match on the source MAC addresses of the packets
src-port	Perform a match on the source port numbers of the packets
vlan-id	Perform a match on the VLAN numbers of the packets

Table 6-6 Operators

Operator	Description
equal	The value of *matched-value* is equal to that of the corresponding field of the packet.
not-equal	The value of *matched-value* is not equal to that of the corresponding field of the packet.
greater-equal	The value of *matched-value* is greater than or equal to that of the corresponding field of the packet.
less-equal	The value of *matched-value* is less than or equal to that of the corresponding field of the packet.
exist	The corresponding packet field exists.
not-exist	The corresponding packet field does not exist.

Description

Use the **uni classification-marking** command to map packets to different priority queues based on the configured keywords.

Use the **undo uni classification-marking** command to remove the configuration.

Examples

Set the priority of packets whose destination MAC address is 000F-E2D7-925A to 3.

```
<Sysname> system-view
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] uni 1 classification-marking index 1 queue 3 priority 3 dst-mac equal
000F-E2D7-925A
```

uni port-policy

Syntax

uni *uni-number* **port-policy** { { **inbound** { **cir** *cir-value* **| bucket-depth** *bucket-depth-value* **| extra-burst-size** *ebs-value* }* } | **outbound cir** *cir-value* [**pir** *pir-value*] }

undo uni *uni-number* **port-policy** { **inbound** | **outbound** }

View

ONU port view

Default Level

2: System level

Parameters

uni-number: UNI number, in the range 1 to the number of UNI ports of the current ONU. The number of UNIs can be up to 80.

inbound: Configure the traffic policing parameters for inbound packets on the UNI port.

cir-value: Committed information rate (CIR) value – guaranteed bandwidth, in the range 0 to 1024000 Kbps. It must be a multiple of 64 and defaults to 102400.

bucket-depth-value: Bucket depth – the maximum burst bandwidth, in the range 1522 to 65535 bytes. The default is 1522.

ebs-value: Available extra bandwidth when the maximum burst bandwidth is exceeded. It is in the range 0 to 1522 bytes, and the default is 0.

pir-value: Peak information rate, in the range of 1 to 1024000 kbps. It must be a multiple of 64.

outbound: Configure the traffic policing parameters for outbound packets on the UNI port.

Description

Use the **uni port-policing** command to configure the traffic policing parameters for the inbound/outbound packets on a UNI port.

Use the **undo uni port-policy** command to restore the traffic policing parameters for the inbound/outbound packets on a UNI port to defaults.

By default, no traffic policing parameter is configured for a UNI.

Examples

Configure the traffic policing parameters for UNI 1.

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

```
[Sysname] interface onu 2/0/1:1
[Sysname-Onu2/0/1:1] uni 1 port-policy inbound cir 25600 bucket-depth 5608 extra-burst-size
800
```

Security Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The Security Volume is organized as follows:

Features	Description
AAA	Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management. This document introduces the commands for AAA configuration.
802.1X	IEEE 802.1X (hereinafter simplified as 802.1X) is a port-based network access control protocol that is used as the standard for LAN user access authentication. This document introduces the commands for 802.1X configuration.
MAC Authentication	MAC authentication provides a way for authenticating users based on ports and MAC addresses; it requires no client software to be installed on the hosts. This document introduces the commands for MAC Authentication configuration.
Portal	Portal authentication, as its name implies, helps control access to the Internet. This document introduces the commands for Portal configuration.
Port Security	Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1X authentication and MAC authentication. This document introduces the commands for Port Security configuration.
IP Source Guard	By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. This document introduces the commands for IP Source Guard configuration.
SSH2.0	SSH ensures secure login to a remote device in a non-secure network environment. By encryption and strong authentication, it protects the device against attacks. This document introduces the commands for SSH2.0 configuration.
ACL	An ACL is used for identifying traffic based on a series of preset matching criteria. This document introduces the commands for ACL configuration.

Table of Contents

1 AAA Configuration Commands

AAA Configuration Commands

access-limit

Syntax

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

View

ISP domain view

Default Level

2: System level

Parameters

disable: Specifies that the system does not limit the number of access users in the current ISP domain.

enable *max-user-number*: Specifies that the system limits the number of access users in the current ISP domain. *max-user-number* is the maximum number of access users in the current ISP domain. The valid range from 1 to 4094.

Description

Use the **access-limit enable** command to set the maximum number of access users allowed by an ISP domain. After the number of user connections reaches the maximum number allowed, no more users will be accepted.

Use the **undo access-limit** or **access-limit disable** command to remove the limitation.

By default, there is no limit to the amount of access users in an ISP domain.

As the access users may compete for network resources, setting a proper limit to the number of access users helps provide a reliable system performance.

Examples

Set a limit of 500 access users for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

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 specify the default accounting scheme for all types of users.

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

By default, the accounting scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The accounting scheme specified 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.
- With the access mode of login, accounting is not supported for FTP services.

Related commands: **authentication default**, **authorization default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local accounting scheme 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 to use the local accounting scheme as the backup scheme.

```
<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 specify the accounting scheme for LAN access users.

Use the **undo accounting lan-access** command to restore the default.

By default, the default accounting scheme 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 scheme 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 to use the local accounting scheme as the backup scheme.

```
<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 specify the accounting scheme for login users.

Use the **undo accounting login** command to restore the default.

By default, the default accounting scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local accounting scheme 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 to use the local accounting scheme as the backup scheme.

```
<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, a user that will be disconnected otherwise can use the network resources even when there is no available accounting server or the communication with the current accounting server fails. This command is normally used when authentication is required but accounting is not.
- If you configure the **accounting optional** command for a domain, the device does not send real-time accounting updates for users of the domain any more after accounting fails.
- With the **accounting optional** command configured, the limit on the number of local user connections configured by the **attribute access-limit** command 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
```

accounting portal

Syntax

accounting portal { **none** | **radius-scheme** *radius-scheme-name* }

undo accounting portal

View

ISP domain view

Default Level

2: System level

Parameters

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 portal** command to specify the accounting scheme for portal users.

Use the **undo accounting portal** command to restore the default.

By default, the default accounting scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting default**, **radius scheme**.

Examples

In the default ISP domain **system**, specify the accounting scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting portal radius-scheme rd
```

attribute

Syntax

attribute { **access-limit** *max-user-number* | **idle-cut** *minute* | **ip** *ip-address* | **location** { [**nas-ip** *ip-address*] **port** *slot-number subslot-number port-number* } | **mac** *mac-address* | **vlan** *vlan-id* } *

undo attribute { **access-limit** | **idle-cut** | **ip** | **location** | **mac** |**vlan** } *

View

Local user view

Default Level

2: System level

Parameters

access-limit *max-user-number*: Specifies the maximum number of concurrent users that can log in using the current username, which ranges from 1 to 1024.

idle-cut *minute*: Configures the idle cut function. The idle cut period ranges from 1 to 120, in minutes.

ip *ip-address*: Specifies the IP address of the user.

location: Specifies the port binding attribute of the user.

nas-ip *ip-address*: Specifies the IP address of the port of the remote access server bound by the user. The default is 127.0.0.1, that is, the device itself. This keyword and argument combination is required only when the user is bound to a remote port.

port *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The value of *slot-number* and *subslot-number* both range from 0 to 15. The value of *port-number* ranges from 0 to 255. The ports bound are determined by port number, regardless of port type.

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 **attribute** command to set some of the attributes for a LAN access user.

Use the **undo attribute** command to remove the configuration.

Note that:

- The **attribute access-limit** command for local users is effective only after local accounting scheme is configured.

- The **attribute ip** command for local users is applicable only to the authentication supporting IP address upload, for example, 802.1X authentication. If this command is configured for the authentication that does not support IP address upload, for example, MAC authentication, local authentication may fail.
- The **idle-cut** command in user interface view applies to LAN users only.

Related commands: **display local-user**.

Examples

Set the IP address of local user **user1** to 10.110.50.1.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] attribute ip 10.110.50.1
```

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 specify the default authentication scheme for all types of users.

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

By default, the authentication scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authentication scheme 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 the local authentication scheme 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 to use the local authentication scheme as the backup scheme.

```
<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 specify the authentication scheme for LAN access users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme 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 the local authentication scheme 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 to use the local authentication scheme as the backup scheme.

```
<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 specify the authentication scheme for login users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme 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 the local authentication scheme 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 to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

authentication portal

Syntax

authentication portal { **none** | **radius-scheme** *radius-scheme-name* }

undo authentication portal

View

ISP domain view

Default Level

2: System level

Parameters

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 portal** command to specify the authentication scheme for portal users.

Use the **undo authentication portal** command to restore the default.

By default, the default authentication scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **radius scheme**.

Examples

In the default ISP domain **system**, specify the authentication scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication portal radius-scheme rd
```

authorization command

Syntax

authorization command hwtacacs-scheme *hwtacacs-scheme-name*

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.

Description

Use the **authorization command** command to specify the authorization scheme for command line users.

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

By default, the default authorization scheme is used for command line users.

Note that the HWTACACS scheme specified for the current ISP domain must have been configured.

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
```

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 specify the authorization scheme for all types of users.

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

By default, the authorization scheme 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 scheme 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. 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 the local authorization scheme 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 to use the local authorization scheme as the backup scheme.

```
<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 right.

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 specify the authorization scheme for LAN access users.

Use the **undo authorization lan-access** command to restore the default.

By default, the default authorization scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authorization default**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local authorization scheme 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 to use the local authorization scheme as the backup scheme.

```
<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 right.

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 specify the authorization scheme for login users.

Use the **undo authorization login** command to restore the default.

By default, the default authorization scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: **authorization default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local authorization scheme 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 to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

authorization portal

Syntax

authorization portal { **none** | **radius-scheme** *radius-scheme-name* }

undo authorization portal

View

ISP domain view

Default Level

2: System level

Parameters

none: None authorization, which means the user is trusted completely. Here, the user is assigned with the default privilege.

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 portal** command to specify the authorization scheme for portal users.

Use the **undo authorization portal** command to restore the default.

By default, the default authorization scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authorization default**, **radius scheme**.

Examples

In the default ISP domain **system**, specify the authorization scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
```

```
[Sysname-isp-system] authorization portal radius-scheme rd
```

cut connection

Syntax

cut connection { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **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.
- **portal**: Specifies portal 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 range 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.

vlan *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies the connections on a slot.

Description

Use the **cut connection** command to tear down the specified connecitons forcibly.

At present, this command applies to only LAN access and portal 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** | **portal** } | **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 { **dot1x** | **mac-authentication** | **portal** }: Specifies user connections of an access mode, that is, 802.1X user connections, MAC authentication user connections, or portal 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 all user connections using the specified IP address.

mac *mac-address*: Specifies all user connections using the specified 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 range 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.

vlan *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies the connections on a slot.

Description

Use the **display connection** command to display information about specified or all AAA user connections.

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**, **domain**, **state**.

Examples

Display the configuration information of all ISP domains.

```
<Sysname> display domain
0  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

1  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

Default Domain Name: system
Total 2 domain(s)
```

Table 1-2 display domain command output description

Field	Description
Domain	Domain name
State	Status of the domain (active or block)
Access-limit	Limit on the number of access users
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication scheme
Default authorization scheme	Default authorization scheme
Default accounting scheme	Default accounting scheme
Lan-access authentication scheme	Authentication scheme for LAN users
Lan-access authorization scheme	Authentication scheme for LAN users
Lan-access accounting scheme	Accounting scheme 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, 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 in the slot where the interface card is inserted.

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 card installed on slot 1.

```
<Sysname> display local-user user-name bbb slot 0
Slot:  0
The contents of local user bbb:
 State:                    Active
 ServiceType:              lan-access
 Idle-cut:                 Disable
 Access-limit:             Enable            Current AccessNum: 100
 Bind location:            Disable
 Vlan ID:                  Disable
 IP address:               Disable
 MAC address:              Disable
FTP Directory:            flash:
User Privilege:           0
Total 1 local user(s) matched.
```

Table 1-3 display local-user command output description (for distributed device)

Field	Description
Slot	Slot number of the card
State	Status of the local user, active or block
ServiceType	Service types that the user can use, including ftp, lan-access, ssh, telnet, and terminal.
Idle-cut	Whether idle cut is enabled
Access-limit	Access user connection limit

Field	Description
Current AccessNum	Number of users currently accessing network services, either for all cards or for a specified card.
Bind location	Whether bound with a port
VLAN ID	VLAN to which the user belongs
IP address	IP address of the user
MAC address	MAC address of the user
FTP Directory	Directory accessible to the FTP user
User Privilege	Local user level
Total 1 local user(s) matched.	1 local user in total

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

Syntax

domain default { **disable** | **enable** *isp-name* }

View

System view

Default Level

3: Manage level

Parameters

disable: Restores the specified default ISP domain to a non-default one.

enable: Configures the specified ISP domain as the default one.

isp-name: Name of the ISP, a string of 1 to 24 characters.

Description

Use the **domain default** command to manually configure the system default ISP domain.

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.
- The default domain configured cannot be deleted unless you cancel it as a default domain first.

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
```

idle-cut

Syntax

idle-cut { **disable** | **enable** *minute* }

View

ISP domain view

Default Level

2: System level

Parameters

disable: Disables the idle cut function.

enable *minute*: Enables the idle cut function. The *minute* argument refers to the allowed idle duration, in the range 1 to 120 minutes.

Description

Use the **idle-cut** command to enable or disable the idle cut function.

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
```

level

Syntax

level *level*

undo level

View

Local user view

Default Level

3: Manage level

Parameters

level: Level of the user, 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.

Description

Use the **level** command to set the level of a user.

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

By default, the user level is 0.

Note that:

- If you specify not to perform authentication or use password authentication, the level of the commands that a user can use after logging in depends on the level of the user interface. For details about the authentication, refer to command **authentication-mode** in *User Interface Commands* of the *System Volume.*
- If you specify an authentication method that requires the username and password, the level of the commands that a user can use after logging in depends on the level of the user. For an SSH user using RSA public key authentication, the commands that can be used depend on the level configured on the user interface.

Related commands: **local-user**.

Examples

Set the level of user **user1** to 3.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] level 3
```

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, 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

Syntax

self-service-url { **disable** | **enable** *url-string* }

undo self-service-url

View

ISP domain view

Default Level

2: System level

Parameters

disable: Disable the self-service server localization function.

enable *url-string*: Enable the self-service server localization function. The *url-string* argument refers to the URL of the self-service server for changing user password. The URL is a string of 1 to 64 characters that starts with http:// and cannot contain any 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 **self-service-url disable** command or the **undo self-service-url** command to disable the self-service server localization function.

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 { **ssh** | **telnet** | **terminal** } * [**level** *level*]

undo service-type { **ssh** | **telnet** | **terminal** } *

View

Local user view

Default Level

3: Manage level

Parameters

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, AUX port.

level *level*: Sets the user level of a Telnet, terminal, or SSH user. The *level* argument is an integer in the range 0 to 3 and defaults to 0.

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
```

service-type ftp

Syntax

service-type ftp

undo service-type ftp

View

Local user view

Default Level

3: Manage level

Parameters

None

Description

Use the **service-type ftp** command to authorize a user to use the FTP service.

Use the **undo service-type ftp** command to disable a user from using the FTP service.

By default, no service is authorized to a user and anonymous access to FTP service is not allowed. If you authorize a user to use the FTP service but do not specify a directory that the user can access, the user can access the root directory of the device by default.

Related commands: **work-directory**.

Examples

Authorize user **user1** to use the FTP service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type ftp
```

service-type lan-access

Syntax

service-type lan-access

undo service-type lan-access

View

Local user view

Default Level

2: System level

Parameters

None

Description

Use the **service-type lan-access** command to specify the lan-access service for an Ethernet access user, for example 802.1X user.

Use the **undo service-type lan-access** command to remove the lan-access service settings for the user.

By default, no service is authorized to users.

Examples

Specify the lan-access service for a user.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type lan-access
```

state

Syntax

state { **active** | **block** }

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.

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
```

work-directory

Syntax

work-directory *directory-name*

undo work-directory

View

Local user view

Default Level

3: Manage level

Parameters

directory-name: Name of the directory that FTP/SFTP users are authorized to access, a case-insensitive string of 1 to 135 characters.

Description

Use the **work-directory** command to specify the directory accessible to FTP/SFTP users.

Use the **undo work-directory** command to restore the default.

By default, FTP/SFTP users can access the root directory of the device.

Note that:

- The specified directory accessible to users must exist.
- If you use a file system command to delete the specified directory, FTP/SFTP users will no longer access the directory.

- If the specified directory carries information about the slot where the secondary board is inserted, FTP/SFTP users cannot log in after primary-to-secondary switching. It is not recommended to carry slot information when you specify a work directory.

Examples

Specify the directory accessible to FTP/SFTP users.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] work-directory flash:
```

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.

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 slot where the interface card is inserted.

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 main processing unit.

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= Not configured
  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
```

```
  nas-ip address                                    = 10.1.1.1

----------------------------------------------------------------
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
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
nas-ip address	The IP address for the device to use as the source address of the RADIUS packets to be sent to the server
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 slot where the interface card is inserted.

Description

Use the **display radius statistics** command to display statistics about RADIUS packets.

Related commands: **radius scheme**.

Examples

Display statistics about RADIUS packets.

```
<Sysname> display radius statistics
Slot  0:state statistic(total=4096):
     DEAD = 4096      AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 0
 AcctStop = 0          OnLine = 0            Stop = 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
state statistic(total=4096)	state statistic
DEAD	Number of idle users
AuthProc	Number of users waiting for authentication
AuthSucc	Number of users that have passed authentication
AcctStart	Number of users for whom 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
Received and Sent packets statistic	Number of packets sent and received
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
RADIUS received packets statistic	Statistic of packets received by RADIUS
Code	Type of packet
Num	Total number of packets
Err	Number of error packets
Running statistic	Statistics of running packets
RADIUS received messages statistic	Number of messages received by RADIUS

Field	Description
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 packets
PKT acct_timeout	Number of accounting timeout packets
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of responses
Session ctrl pkt	Number of session control packets
Normal author request	Number of normal authorization packets
Succ	Number of successful packets
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Number of messages that have been sent by RAIUDS
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
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. 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 slot where the interface card is inserted.

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 on the interface board in slot 1 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
slot 1
 Slot 1
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.

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 to restore the default.

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.

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.

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.

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 slot where the interface card is inserted.

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 slot where the interface card is inserted.

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 retransmission attempts, in the range 1 to 20.

Description

Use the **retry** command to set the maximum number of RADIUS retransmission attempts.

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

The default value for the *retry-times* argument is 3.

Note that:

- Because 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 time-out time, it will retransmit the RADIUS request. If the number of retransmission 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 retransmission attempts defined by this command refers to the sum of all retransmission attempts sent by the device to the primary server and the secondary server. For example, assume that the maximum number of retransmission 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 retransmission attempts reaches N/2 (if N is an even number) or (N+1)/2 (if N is an odd number).
- The maximum number of retransmission 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.

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.

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:

- If more than one interface of the device is configured with user access authentication functions, the interfaces may use different security policy servers. You can specify up to eight security policy servers for a RADIUS scheme.
- The specified security policy server must be a security policy server or RADIUS server that is correctly configured and working normally. Otherwise, the device will regard it as an illegal server.

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**.

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.

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.

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 { **with-domain** | **without-domain** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

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 userid as one.

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 slot where the interface card is inserted.

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
  Domain-included                   : Yes
  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
Domain-included	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 slot where the interface card is inserted.

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** on the interface board in slot 1.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1 slot 1
 Slot 1
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 interface card in the specified slot.

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 slot where the interface card is inserted.

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 { **with-domain** | **without-domain** }

View

HWTACACS scheme view

Default Level

2: System level

Parameters

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.

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
```

Table of Contents

1 802.1X 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
Proxy trap checker is disabled
Proxy logoff checker is disabled
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
               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 2048 per slot
Total current used 802.1X resource number is 1

GigabitEthernet2/0/1  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Handshake 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 Port-based
  Guest VLAN: 4
  Max number of on-line users is 1024

  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 1-1 display dot1x command output description

Field	Description
Equipment 802.1X protocol is enabled	Indicates whether 802.1X is enabled
CHAP authentication is enabled	Indicates whether CHAP authentication is enabled
Proxy trap checker is disabled	Indicates whether the device is configured to send a trap packet when detecting that a user is trying to log in through a proxy
Proxy logoff checker is disabled	Indicates whether the device is configured to get users offline when they are trying to log in through a proxy

Field	Description
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
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
GigabitEthernet2/0/1 is link-up	Status of port GigabitEthernet 2/0/1
802.1X protocol is disabled	Indicates whether 802.1X is enabled on the port
Proxy trap checker is disabled	Indicates whether the port is configured to send a trap packet when detecting that a user is trying to log in through a proxy
Proxy logoff checker is disabled	Indicates whether the port is configured to get users offline when they are trying to log in through a proxy
Handshake is disabled	Indicates whether handshake 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	802.1X multicast-trigger function state
Mandatory authentication domain	Mandatory authentication domain for users accessing the port
Port Control Type is Port-based	Access control method for the port
Guest VLAN	Guest VLAN configured for the port. **Not configured** will be displayed if no guest VLAN is configured.
Max number of on-line user	Maximum number of users supported on the port
EAPOL Packet	Number of EAPOL packets sent (Tx) or 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

Field	Description
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
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 2/0/1, and GigabitEthernet 2/0/5 to GigabitEthernet 2/0/7.

```
<Sysname> system-view
[Sysname] dot1x interface GigabitEthernet 2/0/1 GigabitEthernet 2/0/5 to GigabitEthernet
2/0/7
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] dot1x
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] interface GigabitEthernet 2/0/5
[Sysname-GigabitEthernet2/0/5] dot1x
[Sysname-GigabitEthernet2/0/5] quit
[Sysname] interface GigabitEthernet 2/0/6
[Sysname-GigabitEthernet2/0/6] dot1x
[Sysname-GigabitEthernet2/0/6] quit
[Sysname] interface GigabitEthernet 2/0/7
[Sysname-GigabitEthernet2/0/7] 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 *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.

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 guest VLAN to take effect.
- When the port access control method is set to **portbased**, you can specify a tagged VLAN as the guest VLAN of a Hybrid port, but the guest VLAN does not take effect. If the guest VLAN of a Hybrid port is in operation, you cannot configure the guest VLAN to carry VLAN tag.
- A super VLAN cannot be set as the guest VLAN. Similarly, a guest VLAN cannot be set as the super VLAN. For information about super VLAN, refer to *VLAN Configuration* in the *Access Volume*.
- 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 2/0/1 to use VLAN 999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface GigabitEthernet 2/0/1
```

Specify ports GigabitEthernet 2/0/2 to GigabitEthernet 2/0/5 to use VLAN 10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface GigabitEthernet 2/0/2 to GigabitEthernet 2/0/5
```

Specify all ports to use VLAN 7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

Specify port GigabitEthernet 2/0/7 to use VLAN 3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/7
[Sysname-GigabitEthernet2/0/7] 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:

- The 802.1X proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.
- To ensure that the online user handshake function can work normally, you are recommended to use the iNode client software.

Examples

Enable online user handshake.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/4
[Sysname-GigabitEthernet2/0/4] 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 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] dot1x mandatory-domain my-domain
```

After 802.1X user **usera** passes the authentication, display the user connection information on GigabitEthernet 2/0/1.

```
[Sysname-GigabitEthernet2/0/1] display connection interface GigabitEthernet 2/0/1

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, in the range 1 to 1024.

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 2/0/1 to support simultaneously as 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface GigabitEthernet 2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 GigabitEthernet2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet2/0/1
[Sysname- GigabitEthernet2/0/1] 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 2/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface GigabitEthernet 2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface GigabitEthernet 2/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 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 supp-proxy-check

Syntax

In system view:

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

In Ethernet interface view:

dot1x supp-proxy-check { **logoff** | **trap** }

undo dot1x supp-proxy-check { **logoff** | **trap** }

View

System view, Ethernet interface view

Default Level

2: System level

Parameters

logoff: Gets offline any user trying to log in through a proxy.

trap: Sends a trap to the network management system when detecting that a user is trying to log in through a proxy.

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 supp-proxy-check** command to enable detection and control of users logging in through proxies for specified or all ports.

Use the **undo dot1x supp-proxy-check** command to disable the function for specified or all ports.

By default, the function is disabled.

Note that:

- This function requires the cooperation of the iNode client program.
- In system view, this command enables detection and control of users' login for all ports with *interface-list* not provided, and enables detection and control of users' login for specified ports with *interface-list* provided.
- In Ethernet interface view, you cannot specify the *interface-list* argument and can only enable detection and control of users' login for the current port.
- This function must be enabled both globally in system view and for the intended ports in system view or Ethernet interface view. Otherwise, it does not work.

Related commands: **display dot1x**.

Examples

Specify ports GigabitEthernet 2/0/1 to 1/8 to get users offline when they are trying to log in through proxies.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface GigabitEthernet 2/0/1 to GigabitEthernet 2/0/8
```

Specify port GigabitEthernet 2/0/9 to send a trap packet when detecting that a user is trying to log in through a proxy.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface GigabitEthernet 2/0/9
```

Or

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] interface GigabitEthernet 2/0/9
[Sysname-GigabitEthernet2/0/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-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.

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 10 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.
- 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 2/0/1.

```
<Sysname> reset dot1x statistics interface GigabitEthernet 2/0/1
```

2 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 four now..

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
```

Table of Contents

1 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 2048 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
GigabitEthernet2/0/1 is link-up
```

```
  MAC address authentication is enabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
MAC Addr         Authenticate state          AuthIndex
```

……(part of the output omitted)

Table 1-1 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
GigabitEthernet2/0/1 is link-up	Status of the link on port GigabitEthernet 2/0/1
MAC address authentication is enabled	Whether MAC authentication is enabled on port GigabitEthernet 2/0/1
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.
AuthIndex	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 2/0/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 2/0/1
Mac-auth is enabled on port GigabitEthernet2/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet2/0/1.
```

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 2/0/1.

```
<Sysname> reset mac-authentication statistics interface GigabitEthernet 2/0/1
```

Table of Contents

1 Portal Configuration Commands

Note

EA series cards, LSQ1GP12EA and LSQ1TGX1EA for example, do not support Portal authentication.

Portal Configuration Commands

display portal acl

Syntax

display portal acl { **all** | **dynamic** | **static** } **interface** *interface-type interface-number*

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all portal access control lists (ACLs), including dynamic ones and static ones.

dynamic: Displays dynamic portal ACLs, namely, ACLs generated after a user passes portal authentication.

static: Displays static portal ACLs, namely, ACLs generated by related configurations.

interface *interface-type interface-number*: Displays the ACLs on the specified interface.

Description

Use the **display portal acl** command to display the ACLs on a specified interface.

Examples

Display all ACLs on interface Vlan-interface 2.

```
<Sysname> display portal acl all interface Vlan-interface 2
Vlan-interface2 portal ACL rule:
 Rule 0
 Inbound interface = Vlan-interface2
 Type            = static
 Action          = permit
 Source:
```

```
    IP       = 0.0.0.0
    Mask     = 0.0.0.0
    MAC      = 0000-0000-0000
    Interface = any
    VLAN     = 0
    Protocol  = 0
  Destination:
    IP       = 192.168.0.111
    Mask     = 255.255.255.255

Rule 1
  Inbound interface = Vlan-interface2
  Type            = static
  Action           = redirect
  Source:
    IP       = 0.0.0.0
    Mask     = 0.0.0.0
    MAC      = 0000-0000-0000
    Interface = any
    VLAN     = 2
    Protocol  = 6
  Destination:
    IP       = 0.0.0.0
    Mask     = 0.0.0.0

  Rule 2
  Inbound interface = Vlan-interface2
  Type            = dynamic
  Action           = permit
  Source:
    IP       = 2.2.2.2
    Mask     = 255.255.255.255
    MAC      = 000d-88f8-0eab
    Interface = GigabitEthernet5/0
    VLAN     = 0
    Protocol  = 0
  Destination:
    IP       = 0.0.0.0
    Mask     = 0.0.0.0
Author ACL:
    Number   = 3001
```

Table 1-1 display portal acl command output description

Field	Description
Rule	Sequence number of the generated ACL, which is numbered from 0 in ascending order
Inbound interface	Interface to which portal ACLs are bound

Field	Description
Type	Type of the portal ACL
Action	Match action in the portal ACL
Source	Source information in the portal ACL
IP	Source IP address in the portal ACL
Mask	Subnet mask of the source IP address in the portal ACL
MAC	Source MAC address in the portal ACL
Interface	Source interface in the portal ACL
VLAN	Source VLAN in the portal ACL
Protocol	Protocol type in the portal ACL
Destination	Destination information in the portal ACL
IP	Destination IP address in the portal ACL
Mask	Subnet mask of the destination IP address in the portal ACL
Author ACL	Authorization ACL of portal ACL. It is displayed only when the Type field has a value of dynamic.
Number	Authorization ACL number assigned by the server. None indicates that the server did not assign any ACL.

display portal connection statistics

Syntax

display portal connection statistics { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all interfaces.

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

Description

Use the **display portal connection statistics** command to display portal connection statistics on a specified interface or all interfaces.

Examples

Display portal connection statistics on interface Vlan-interface 2.

```
<Sysname> display portal connection statistics interface Vlan-interface 2
 ---------------Interface: Vlan-interface2----------------------
 User state statistics:
```

State-Name	User-Num
VOID	0
DISCOVERED	0
WAIT_AUTHEN_ACK	0
WAIT_AUTHOR_ACK	0
WAIT_LOGIN_ACK	0
WAIT_ACL_ACK	0
WAIT_NEW_IP	0
WAIT_USERIPCHANGE_ACK	0
ONLINE	1
WAIT_LOGOUT_ACK	0
WAIT_LEAVING_ACK	0

Message statistics:

Msg-Name	Total	Err	Discard
MSG_AUTHEN_ACK	3	0	0
MSG_AUTHOR_ACK	3	0	0
MSG_LOGIN_ACK	3	0	0
MSG_LOGOUT_ACK	2	0	0
MSG_LEAVING_ACK	0	0	0
MSG_CUT_REQ	0	0	0
MSG_AUTH_REQ	3	0	0
MSG_LOGIN_REQ	3	0	0
MSG_LOGOUT_REQ	2	0	0
MSG_LEAVING_REQ	0	0	0
MSG_ARPPKT	0	0	0
MSG_TMR_REQAUTH	1	0	0
MSG_TMR_AUTHEN	0	0	0
MSG_TMR_AUTHOR	0	0	0
MSG_TMR_LOGIN	0	0	0
MSG_TMR_LOGOUT	0	0	0
MSG_TMR_LEAVING	0	0	0
MSG_TMR_NEWIP	0	0	0
MSG_TMR_USERIPCHANGE	0	0	0
MSG_PORT_REMOVE	0	0	0
MSG_VLAN_REMOVE	0	0	0
MSG_IF_REMOVE	6	0	0
MSG_L3IF_SHUT	0	0	0
MSG_IP_REMOVE	0	0	0
MSG_ALL_REMOVE	1	0	0
MSG_IFIPADDR_CHANGE	0	0	0
MSG_SOCKET_CHANGE	8	0	0
MSG_NOTIFY	0	0	0
MSG_SETPOLICY	0	0	0
MSG_SETPOLICY_RESULT	0	0	0

Table 1-2 display portal connection statistics command output description

Field	Description
User state statistics	Statistics on portal users
State-Name	Name of a user state
User-Num	Number of users
VOID	Number of users in void state
DISCOVERED	Number of users in discovered state
WAIT_AUTHEN_ACK	Number of users in wait_authen_ack state
WAIT_AUTHOR_ACK	Number of users in wait_author_ack state
WAIT_LOGIN_ACK	Number of users in wait_login_ack state
WAIT_ACL_ACK	Number of users in wait_acl_ack state
WAIT_NEW_IP	Number of users in wait_new_ip state
WAIT_USERIPCHANGE_ACK	Number of users wait_useripchange_ack state
ONLINE	Number of users in online state
WAIT_LOGOUT_ACK	Number of users in wait_logout_ack state
WAIT_LEAVING_ACK	Number of users in wait_leaving_ack state
Message statistics	Statistics on messages
Msg-Name	Message type
Total	Total number of messages
Err	Number of erroneous messages
Discard	Number of discarded messages
MSG_AUTHEN_ACK	Authentication acknowledgment message
MSG_AUTHOR_ACK	Authorization acknowledgment message
MSG_LOGIN_ACK	Accounting acknowledgment message
MSG_LOGOUT_ACK	Accounting-stop acknowledgment message
MSG_LEAVING_ACK	Leaving acknowledgment message
MSG_CUT_REQ	Cut request message
MSG_AUTH_REQ	Authentication request message
MSG_LOGIN_REQ	Accounting request message
MSG_LOGOUT_REQ	Accounting-stop request message
MSG_LEAVING_REQ	Leaving request message
MSG_ARPPKT	ARP message
MSG_TMR_REQAUTH	Authentication request timeout message
MSG_TMR_AUTHEN	Authentication timeout message
MSG_TMR_AUTHOR	Authorization timeout message
MSG_TMR_LOGIN	Accounting-start timeout message
MSG_TMR_LOGOUT	Accounting-stop timeout message

Field	Description
MSG_TMR_LEAVING	Leaving timeout message
MSG_TMR_NEWIP	Public IP update timeout message
MSG_TMR_USERIPCHANGE	User IP change timeout message
MSG_PORT_REMOVE	Users-of-a-Layer-2-port-removed message
MSG_VLAN_REMOVE	VLAN user removed message
MSG_IF_REMOVE	Users-of-a-Layer-3-interface-removed message
MSG_L3IF_SHUT	Layer 3 interface shutdown message
MSG_IP_REMOVE	User-with-an-IP-removed message
MSG_ALL_REMOVE	All-users-removed message
MSG_IFIPADDR_CHANGE	Interface IP address change message
MSG_SOCKET_CHANGE	Socket change message
MSG_NOTIFY	Notification message
MSG_SETPOLICY	Set policy message for assigning security ACL
MSG_SETPOLICY_RESULT	Set policy response message

display portal free-rule

Syntax

display portal free-rule [*rule-number*]

View

Any view

Default Level

1: Monitor level

Parameters

rule-number: Number of a portal-free rule. The value range from 0 to 31.

Description

Use the **display portal free-rule** command to display information about a specified portal-free rule or all portal-free rules.

Related commands: **portal free-rule**.

Examples

Display information about portal-free rule 1.

```
<Sysname> display portal free-rule 1
 Rule-Number  1:
 Source:
   IP       = 2.2.2.0
   Mask     = 255.255.255.0
```

```
  MAC      = 0000-0000-0000
  Interface = any
  Vlan     = 0
Destination:
  IP       = 0.0.0.0
  Mask     = 0.0.0.0
```

Table 1-3 display portal free-rule command output description

Field	Description
Rule-Number	Number of the portal-free rule
Source	Source information in the portal-free rule
IP	Source IP address in the portal-free rule
Mask	Subnet mask of the source IP address in the portal-free rule
MAC	Source MAC address in the portal-free rule
Interface	Source interface in the portal-free rule
Vlan	Source VLAN in the portal-free rule
Destination	Destination information in the portal-free rule
IP	Destination IP address in the portal-free rule
Mask	Subnet mask of the destination IP address in the portal-free rule

display portal interface

Syntax

display portal 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 portal interface** command to display the portal configuration of an interface.

Examples

Display the portal configuration of interface Vlan-interface 2.

```
<Sysname> display portal interface Vlan-interface 2
 Interface portal configuration:
 Vlan-interface2: Portal running
 Portal server: servername
```

```
Authentication type: Direct
Authentication network:
address = 0.0.0.0  mask = 0.0.0.0
```

Table 1-4 display portal interface command output description

Field	Description
Interface portal configuration	Portal configuration on the interface
Vlan-interface 2	Status of the portal feature on the interface, disable, enable, or running.
Portal server	Portal server referenced by the interface
Authentication type	Authentication mode enabled on the interface
Authentication network	Information of the portal authentication subnet
address	IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

display portal server

Syntax

display portal server [*server-name*]

View

Any view

Default Level

1: Monitor level

Parameters

server-name: Name of a portal server, a case-sensitive string of 1 to 32 characters.

Description

Use the **display portal server** command to display information about a specified portal server or all portal servers.

Related commands: **portal server**.

Examples

Display information about portal server aaa.

```
<Sysname> display portal server aaa
 Portal server:
  1)aaa:
    IP   = 192.168.0.111
    Key  = portal
    Port = 50100
    URL  = http://192.168.0.111/portal
```

Table 1-5 display portal server command output description

Field	Description
1)	Number of the portal server
aaa	Name of the portal server
IP	IP address of the portal server
Key	Key for portal authentication **Not configured** will be displayed if no key is configured.
Port	Listening port on the portal server
URL	Address the packets are to be redirected to **Not configured** will be displayed if no address is configured.

display portal server statistics

Syntax

display portal server statistics { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all interfaces.

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

Description

Use the **display portal server statistics** command to display portal server statistics on a specified interface or all interfaces.

Note that with the **all** keyword specified, the command displays portal server statistics by interface and therefore statistics about a portal server referenced by more than one interface may be displayed repeatedly.

Examples

Display portal server statistics on Vlan-interface 2.

```
<Sysname> display portal server statistics interface Vlan-interface 2
 ---------------Interface: Vlan-interface2----------------------
 Server name:  st
 Invalid packets: 0
 Pkt-Name                      Total   Discard  Checkerr
 REQ_CHALLENGE                   3       0       0
 ACK_CHALLENGE                   3       0       0
 REQ_AUTH                        3       0       0
```

```
ACK_AUTH                    3       0       0
REQ_LOGOUT                  1       0       0
ACK_LOGOUT                  1       0       0
AFF_ACK_AUTH                3       0       0
NTF_LOGOUT                  1       0       0
REQ_INFO                    6       0       0
ACK_INFO                    6       0       0
NTF_USERDISCOVER            0       0       0
NTF_USERIPCHANGE            0       0       0
AFF_NTF_USERIPCHANGE        0       0       0
ACK_NTF_LOGOUT              1       0       0
```

Table 1-6 display portal server statistics command output description

Field	Description
Interface	Interface referencing the portal server
Server name	Name of the portal server
Invalid packets	Number of invalid packets
Pkt-Name	Packet type
Total	Total number of packets
Discard	Number of discarded packets
Checkerr	Number of erroneous packets
REQ_CHALLENGE	Challenge request message the portal server sends to the access device
ACK_CHALLENGE	Challenge acknowledgment message the access device sends to the portal server
REQ_AUTH	Authentication request message the portal server sends to the access device
ACK_AUTH	Authentication acknowledgment message the access device sends to the portal server
REQ_LOGOUT	Logout request message the portal server sends to the access device
ACK_LOGOUT	Logout acknowledgment message the access device sends to the portal server
AFF_ACK_AUTH	Affirmation message the portal server sends to the access device after receiving an authentication acknowledgement message
NTF_LOGOUT	Forced logout notification message the access device sends to the portal server
REQ_INFO	Information request message
ACK_INFO	Information acknowledgment message
NTF_USERDISCOVER	User discovery notification message the portal server sends to the access device
NTF_USERIPCHANGE	User IP change notification message the access device sends to the portal server
AFF_NTF_USERIPCHANGE	User IP change success notification message the portal server sends to the access device

Field	Description
ACK_NTF_LOGOUT	Forced logout acknowledgment message from the portal server

display portal tcp-cheat statistics

Syntax

display portal tcp-cheat statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display portal tcp-cheat statistics** command to display TCP spoofing statistics.

Examples

Display TCP spoofing statistics.

```
<Sysname> display portal tcp-cheat statistics
 TCP Cheat Statistic:
 Total Opens: 0
 Resets Connections: 0
 Current Opens: 0
 Packets Received: 0
 Packets Sent: 0
 Packets Retransmitted: 0
 Packets Dropped: 0
 HTTP Packets Sent: 0
 Connection State:
        SYN_RECVD: 0
        ESTABLISHED: 0
        CLOSE_WAIT: 0
        LAST_ACK: 0
        FIN_WAIT_1: 0
        FIN_WAIT_2: 0
        CLOSING: 0
```

Table 1-7 display portal tcp-cheat statistics command output description

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections

Field	Description
Resets Connections	Number of connections reset through RST packets
Current Opens	Number of connections currently being setting up
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of HTTP packets sent
Connection State	Statistics of connections in various state
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

display portal user

Syntax

display portal user { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Specifies all interfaces.

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

Description

Use the **display portal user** command to display information about portal users on a specified interface or all interfaces.

Examples

Display information about portal users on all interfaces.

```
<Sysname> display portal user all
 Index:2
 State:ONLINE
 SubState:INVALID
 ACL:NONE
```

```
MAC             IP              Vlan   Interface
--------------------------------------------------------------------------
000d-88f8-0eab  2.2.2.2         0      Vlan-interface2
Index:3
State:ONLINE
SubState:INVALID
ACL:3000
MAC             IP              Vlan   Interface
--------------------------------------------------------------------------
000d-88f8-0eac  2.2.2.3         0      Vlan-interface2
Total 2 user(s) matched, 2 listed.
```

Table 1-8 display portal user command output description

Field	Description
Index	Index of the portal user
State	Current status of the portal user
SubState	Current sub-status of the portal user
ACL	Authorization ACL of the portal user
MAC	MAC address of the portal user
IP	IP address of the portal user
Vlan	VLAN to which the portal user belongs
Interface	Interface to which the portal user is attached
Total 2 user(s) matched, 2 listed	Total number of portal users

portal auth-network

Syntax

portal auth-network *network-address* { *mask-length* | *mask* }

undo portal auth-network { *network-address* | **all** }

View

Interface view

Default Level

2: System level

Parameters

network-address: IP address of the authentication subnet.

mask-length: Length of the subnet mask, in the range of 0 to 32.

mask: Subnet mask, in dotted decimal notation.

all: Specifies all authentication subnets.

Description

Use the **portal auth-network** command to configure a portal authentication subnet.

Use the **undo portal auth-network** command to remove a specified portal authentication subnet or all portal authentication subnets.

Note that this command is only applicable for Layer 3 authentication. The portal authentication subnet for direct authentication is any source IP address, and the portal authentication subnet for re-DHCP authentication is the one determined by the private IP address of the interface.

By default, the portal authentication subnet is 0.0.0.0/0, meaning that users in all subnets are to be authenticated.

Examples

Configure a portal authentication subnet of 10.10.10.0/24.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 1
[Sysname- Vlan-interface1] portal auth-network 10.10.10.0 24
```

portal delete-user

Syntax

portal delete-user { *ip-address* | **all** | **interface** *interface-type interface-number* }

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of a user.

all: Logs out all users.

interface *interface-type interface-number*: Logs out all users on the specified interface.

Description

Use the **portal delete-user** command to log out users.

Related commands: **display portal user**.

Examples

Log out user 1.1.1.1.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

portal free-rule

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } | **source** { **any** | [**interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } | **mac** *mac-address* | **vlan** *vlan-id*] * } } *

undo portal free-rule { *rule-number* | **all** }

View

System view

Default Level

2: System level

Parameters

rule-number: Number for the portal-free rule. The value range from 0 to 31.

any: Imposes no limitation on the previous keyword.

ip *ip-address*: Specifies an IP address.

mask { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range 0 to 32.

interface *interface-type interface-number*: Specifies a source interface.

mac *mac-address*: Specifies a source MAC address in the format of H-H-H.

vlan *vlan-id*: Specifies a source VLAN ID.

all: Specifies all portal-free rules.

Description

Use the **portal free-rule** command to configure a portal-free rule and specify the source filtering condition and/or destination filtering condition.

Use the **undo portal free-rule** command to remove a specified portal-free rule or all portal-free rules.

Note that:

- If you specify both the source IP address and source MAC address, the IP address must be a host address under a 32-bit mask. Otherwise, the specified MAC address does not take effect.
- If you specify both a VLAN and interface in a portal-free rule, the interface must belong to the VLAN.
- You cannot configure a portal-free rule to have the same filtering criteria as that of an existing one. Otherwise, the system prompts that the rule already exists.
- No matter whether portal authentication is enabled, you can only add or remove a portal-free rule, rather than modifying it.

Related commands: **display portal free-rule**.

Note

- If you specify both the source IP and source MAC address information in a portal-free rule, the IP address must be a host address with a mask of 32 bits; otherwise, the specified MAC address will be neglected.
- You cannot configure two portal-free rules with the same filtering conditions. Otherwise, the device will prompt that the portal-free rule already exists.

Examples

Configure a portal-free rule, allowing any packet whose source IP address is 10.10.10.1/24 and source interface is GigabitEthernet 2/0/1 to bypass portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 15 source ip 10.10.10.1 mask 24 interface GigabitEthernet 2/0/1
destination ip any
```

portal server

Syntax

portal server *server-name* **ip** *ip-address* [**key** *key-string* | **port** *port-id* | **url** *url-string*] *

undo portal server *server-name* [**key** | **port** | **url**]

View

System view

Default Level

2: System level

Parameters

server-name: Name of the portal server, a case-sensitive string of 1 to 32 characters.

ip-address: IP address of the portal server.

key-string: Shared key for communication with the portal server, a case-sensitive string of 1 to 16 characters.

port-id: Destination port number used when the device sends a message to the portal server unsolicitedly, in the range 1 to 65534. The default is 50100.

url-string: Uniform resource locator (URL) to which HTTP packets are to be redirected, in the *http://ip-address* format. The default of *ip-address* is the IP address of the portal server.

Description

Use the **portal server** command to configure a portal server.

Use the **undo portal server** command to remove a portal server, restore the default destination port number or URL, or delete the shared key.

By default, no portal server is configured.

Note that:

- Using the **undo portal server** *server-name* command, you remove the specified portal server if the specified portal server exists and there is no user on the interfaces referencing the portal server.
- The configured portal server and its parameters can be removed or modified only when the portal server is not referenced by an interface.
- To remove or modify the settings of a portal server that has been referenced by an interface, you must remove the portal configuration on the interface using the **undo portal** command.

Related commands: **display portal server**.

Examples

Configure portal server **pts**, setting the IP address to 192.168.0.111, the key to portal, and the redirection URL to http://192.168.0.111/portal.

```
<Sysname> system-view
[Sysname] portal server pts ip 192.168.0.111 key portal url http://192.168.0.111/portal
```

portal server method

Syntax

portal server *server-name* **method** { **direct** | **layer3** | **redhcp** }

undo portal

View

Interface view

Default Level

2: System level

Parameters

server-name: Name of the portal server, a case-sensitive string of 1 to 32 characters.

method: Specifies the authentication mode to be used.

direct: Direct authentication.

layer3: Layer 3 authentication.

redhcp: Re-DHCP authentication.

Description

Use the **portal server** command to enable portal authentication on an interface, and specify the portal server to be referenced and the authentication mode.

Use the **undo portal** command to disable portal authentication on an interface.

By default, portal authentication is disabled on an interface.

Note that: The portal server to be referenced must exist.

Related commands: **display portal server**.

Examples

Enable portal authentication on interface VLAN-interface 100, setting the portal server to **pts**, and the authentication mode to **direct**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal server pts method direct
```

reset portal connection statistics

Syntax

reset portal connection statistics { **all** | **interface** *interface-type interface-number* }

View

User view

Default Level

1: Monitor level

Parameters

all: Specifies all interfaces.

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

Description

Use the **reset portal connection statistics** command to clear portal connection statistics on a specified interface or all interfaces.

Examples

Clear portal connection statistics on interface Vlan-interface 1.

```
<Sysname> reset portal connection statistics interface Vlan-interface 1
```

reset portal server statistics

Syntax

reset portal server statistics { **all** | **interface** *interface-type interface-number* }

View

User view

Default Level

1: Monitor level

Parameters

all: Specifies all interfaces.

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

Description

Use the **reset portal server statistics** command to clear portal server statistics on a specified interface or all interfaces.

Examples

Clear portal server statistics on interface Vlan-interface 1.

```
<Sysname> reset portal server statistics interface Vlan-interface 1
```

reset portal tcp-cheat statistics

Syntax

reset portal tcp-cheat statistics

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **reset portal tcp-cheat statistics** command to clear TCP spoofing statistics.

Examples

Clear TCP spoofing statistics.

```
<Sysname> reset portal tcp-cheat statistics
```

Table of Contents

1 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

GigabitEthernet2/0/1 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
GigabitEthernet2/0/2 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 1-1 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      GigabitEthernet2/0/1       1
000d-88f8-0577      GigabitEthernet2/0/2       1
  ---  2 mac address(es) found  ---
```

Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count
  ---  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      GigabitEthernet2/0/1        1
000d-88f8-0577      GigabitEthernet2/0/2        1
  ---  2 mac address(es) found  ---
```

Display information about all blocked MAC addresses of port GigabitEthernet 2/0/2.

```
<Sysname> display port-security mac-address block interface GigabitEthernet 2/0/2
MAC ADDR             From Port                 VLAN ID
000d-88f8-0577      GigabitEthernet2/0/2       1
  ---  1 mac address(es) found  ---
```

Display information about all blocked MAC addresses of port GigabitEthernet 2/0/2 in VLAN 1.

```
<Sysname> display port-security mac-address block interface GigabitEthernet2/0/2 vlan 1
MAC ADDR             From Port                  VLAN ID
000d-88f8-0577       GigabitEthernet2/0/2       1
  ---  1 mac address(es) found  ---
```

Table 1-2 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          GigabitEthernet2/0/1      NOAGED
```

```
000d-88f8-0577  1      Security          GigabitEthernet2/0/2      NOAGED

  ---  2 mac address(es) found  ---
```

Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address security 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       GigabitEthernet2/0/1     NOAGED
000d-88f8-0577  1       Security       GigabitEthernet2/0/2     NOAGED

  ---  2 mac address(es) found  ---
```

Display information about secure MAC addresses on the specified port.

```
<Sysname> display port-security mac-address security interface GigabitEthernet2/0/2
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
000d-88f8-0577  1       Security        GigabitEthernet2/0/2     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 2/0/2 vlan
1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
000d-88f8-0577  1       Security       GigabitEthernet2/0/2          NOAGED

  ---  1 mac address(es) found  ---
```

Table 1-3 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
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

Ethernet port 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 2/0/1 to ignore the authorization information from the RADIUS server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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

Ethernet port 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** 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 2/0/1 to block the source MAC addresses of illegal frames after intrusion protection is triggered.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port-security intrusion-mode blockmac
```

port-security mac-address security

Syntax

In Ethernet port 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

Ethernet port 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 2/0/1 to autoLearn, and add a secure MAC address of 0001-0001-0002 (belonging to VLAN 10) for port GigabitEthernet 2/0/1 in system view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet2/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet 2/0/1
vlan 10
```

Enable port security, set the port security mode of port GigabitEthernet 2/0/1 to autoLearn, and add a secure MAC address of 0001-0002-0003 (belonging to VLAN 4) for port GigabitEthernet 2/0/1 in interface view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet2/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 frames destined for authenticated MAC addresses or the broadcast address.

ntk-withmulticasts: Sends frames destined for authenticated MAC addresses, the broadcast address, or unknown multicast addresses.

ntkonly: Sends 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.

The frames checked by the NTK feature include the authenticated unicasts, broadcasts, and frames destined for unknown multicast addresses. Frames destined for known multicast addresses are not checked.

Related commands: **display port-security**.

Examples

Set the NTK mode of port GigabitEthernet 2/0/1 to **ntkonly**, allowing the port to forward received packets to only devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1 as secure.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port-security port-mode secure
```

Change the port security mode of port GigabitEthernet 2/0/1 to userLogin.

```
[Sysname-GigabitEthernet2/0/1] undo port-security port-mode
[Sysname-GigabitEthernet2/0/1] 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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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
```

Table of Contents

1 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: 3
  MAC                 IP          Vlan       Port               Status
  040a-0000-4000      10.1.0.9    2          Ethernet2/0/1      DHCP-SNP
  N/A                 10.1.0.8    2          Ethernet2/0/1      DHCP-SNP
  040a-0000-2000      10.1.0.7    2          Ethernet2/0/1      DHCP-SNP
```

Table 1-1 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    Ethernet2/0/1               Static
 0001-0001-0001    2.2.2.2         N/A    Ethernet2/0/1               Static
 0003-0003-0003    N/A             N/A    Ethernet2/0/1               Static
 0004-0004-0004    4.4.4.4         N/A    Ethernet2/0/1               Static
```

Table 1-2 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	Static binding entry does not support VLAN-port 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.

Examples

Configure dynamic binding function on port Ethernet 2/0/1 to filter packets based on both source IP address and MAC address.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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* }

undo user-bind { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* }

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.

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. A binding entry can be configured to multiple ports.
- 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0001-0001
```

Table of Contents

1 SSH2.0 Configuration Commands

SSH2.0 Configuration Commands

display public-key local

Syntax

display public-key local rsa public

View

Any view

Default Level

1: Monitor level

Parameters

rsa: Displays the public key of the RSA local key pair.

Description

Use the **display public-key local** command to display the information about the public keys of the local key pairs.

Related commands: **public-key local create**.

Examples

Display the public key information of the RSA local key pair.

```
<Sysname> display public-key local rsa public

=====================================================
Time of Key pair created: 19:59:16  2006/10/25
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A63
3BA0F1DB01F84EB51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D04914
3656F1287502C06D39D39F28F0F5CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCD
B5DB620CD1F471401B7117139702348444A2D8900497A87B8D5F13D61C4DEFA3D14A7DC076
24791FC1D226F62DF3020301
0001

=====================================================
Time of Key pair created: 19:59:17  2006/10/25
```

```
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2
AACC7B2AE12B2B1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27
E054BFAA0A85E113FBDE751EE0ECEF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB
5D299D1E4E27A13C7DD10203010001
```

Table 1-1 display public-key local command output description

Field	Description
Time of Key pair created	Time when the key pair is created
Key name	Name of the key
Key type	Type of the key
Key code	Code of the key

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 public keys of SSH peers.

name *publickey-name*: Specifies a public key of an SSH peer by its name, which is a 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 SSH 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 SSH 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 an SSH peer.

Related commands: **public-key peer**, **public-key peer import sshkey**.

Examples

Display detailed information about the locally saved public key named **idrsa**.

```
<Sysname> display public-key peer name idrsa
```

```
=====================================
  Key name  : idrsa
  Key type  : RSA
  Key module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B0030818702818100C46A8710216CEC0
C01C7CE136BA76C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB
39B3F39C5CE56C95B6AB7442D56393BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFF
B58BE6F035FAA2C596B27D1231D159846B7CB9A7757C5800FADA9FD72F65672F4A549EE99F
63095E11BD37789955020123
```

Table 1-2 display public-key peer name command output description

Field	Description
Key name	Name of the key
Key type	Type of the key
Key module	Module of the key
Key code	Code of the key

Display brief information about all locally saved public keys of SSH peers.

```
<Sysname> display public-key peer brief
Type  Module  Name
---------------------------
RSA   1024    idrsa
```

Table 1-3 display public-key peer brief command output description

Field	Description
Type	Type of the key
Module	Number of bits in the key
Name	Name of the public key of an SSH peer

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.

```
<Syaname> display sftp client source
The source IP address you specified is 192.168.0.1
```

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

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**.

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 1-4 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 1-5 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 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**.

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 1-6 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

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**.

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 1-7 display ssh user-information command output description

Field	Description
Username	Name of the user
Authentication-type	Authentication type. 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

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 data. It must be a hexadecimal string that has not been converted and in the distinguished encoding rules (DER) encoding format. Spaces and carriage returns are allowed between characters.

Related commands: **public-key peer**, **public-key-code end**.

Examples

Enter public key code view to 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 illegal characters, the system displays an error message and discards the key. If the key is legal, the system saves it.

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 rsa

View

System view

Default Level

2: System level

Parameters

rsa: RSA key pair.

Description

Use the **public-key local create** command to create a local key pair.

Note that:

- When using this command to create a RSA key pair, you will be prompted to provide the length of the key pair. The length of a server/host key must be in the range 512 to 2048 bits and defaults to 1024. If the key pair already exists, the system will ask you whether you want to overwrite it.
- The configuration of this command can survive a reboot. You only need to configure it once.

Related commands: **public-key local destroy**, **display public-key local**.

Examples

Create an RSA local key pair.

```
<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 may take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating keys...
........++++++
.....................................++++++
.......++++++++
.....................++++++++
.
```

public-key local destroy

Syntax

public-key local destroy rsa

View

System view

Default Level

2: System level

Parameters

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 RSA local key pair.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
```

public-key local export rsa

Syntax

public-key local export rsa { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

Default Level

2: System 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 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 RSA local public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the RSA local public key on the screen; otherwise, the command exports the RSA local public key to the specified file and saves the file.

SSH1, SSH2.0 and OpenSSH are three different public key file formats for different requirements.

Related commands: **public-key local create**, **public-key local destroy**.

Examples

Export the RSA local 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 RSA local public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20061105"
AAAAB3NzaC1yc2EAAAADAQABAAAAgKRkxFoZ+T72Srs9c60+j2yrkd0AHBsXBh0Uq+iNvE12PaYR1On4
x+aNlwe9fjW1PYgzH+DRkTpiMrn3j2pIs7gaJXvefTW94rbVWJ94uiSDk1NLX1JcoTtWnQcVhft3mUZ+
J0jBEhAcw4bROe7/qr6l7VTCo9FBZ0XgKuHroovX
---- END SSH2 PUBLIC KEY ----
```

Display the RSA local public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa       AAAAB3NzaC1yc2EAAAADAQABAAAAgLxMOSqXc0pjO6Dx2wH4TrUSKOyGreHbpZfg2QZv3E8Ed2
zqNhDSV4NB9dBJFDZW8Sh1AsBtOdOfKPD1y6Yw2ozRwW7OinplKC8kB+h1fnk33M2122IM0fRx
QBtxFxOXAjSERKLYkASXqHuNXxPWHE3vo9FKfcB2JHkfwdIm9i3z 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 string of 1 to 64 characters.

Description

Use the **public-key peer** command to enter public key view.

Use the **undo public-key peer** command to remove the configured peer public key.

After entering public key view, you can configure the peer public key 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**.

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 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 a peer public key from the public key file.

Use the **undo public-key peer** command to remove the setting.

After execution of this command, the system automatically transforms the public key file 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/TFTP.

Examples

Import a peer public key named key2 from public key file key.pub.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

sftp

Syntax

sftp *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

3: Manage level

Parameters

server: IPv4 address or name of the server, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **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 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.

Examples

Connect to SFTP server 10.1.1.2.

```
<Sysname> sftp 10.1.1.2
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.

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*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

3: Manage level

Parameters

server: IPv6 address or name of the server, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **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.

Examples

Connect to server 2:5::8:9.

```
<Sysname> sftp ipv6 2:5::8:9
Input Username:
```

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
```

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 enable

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.

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
```

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.

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 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 mode of an SSH user, which can be one the following:

- **password**: Performs password authentication.
- **any**: Performs either password authentication or publickey authentication.
- **password-publickey**: Performs both password authentication and publickey authentication. A client running SSH1 client only needs to pass either type of authentication while a client running SSH2.0 client must pass both types of authentication to log in.
- **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 mode.

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 mode 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 mode. 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 modes, 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 mode 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

Syntax

ssh2 *server* [*port-number*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

0: Visit level

Parameters

server: IPv4 address or name of the server, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.

- **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, the preferred encryption algorithms and HMAC algorithms of the client and the server.

Examples

Log in to remote SSH2.0 server 10.214.50.51, 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 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*] [**prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

0: Visit level

Parameters

server: IPv6 address or name of the server, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **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, the preferred encryption algorithms, and preferred HMAC algorithms of the client and the server.

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 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
```

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
```

Table of Contents

1 ACL Configuration Commands

Common Configuration Commands

display acl resource

Syntax

display acl resource [**slot** *slot-id*]

View

Any view

Default Level

1: Monitor level

Parameters

slot-id: Number of the slot.

Description

Use the **display acl resource** command to display the ACL uses on a switch.

Note that:

- Using the command with a specified a slot will display the ACL uses of that slot. Otherwise, the ACL uses of all slots of the device will be displayed.
- If the board specified by the slot number is not in place or not working normally, this command will display nothing.

Examples

Display the ACL uses of all slots on the switch.

```
<Sysname> display acl resource

 Interface:
    Eth2/0/1 to Eth2/0/24
-------------------------------------------------------------------------
  Type       Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------
 IFP ACL     1024     0         50          974
 IFP Meter   512      0         44          468
 IFP Counter 512      0         0           512

 Interface:
    Eth2/0/25 to Eth2/0/48
-------------------------------------------------------------------------
```

```
 Type       Total   Reserved  Configured  Remaining
------------------------------------------------------------------------------
 IFP ACL     1024     0         46          978
 IFP Meter   512      0         44          468
 IFP Counter 512      0         0           512


 Interface:
    GE3/0/1 to GE3/0/24
------------------------------------------------------------------------------
 Type       Total   Reserved  Configured  Remaining
------------------------------------------------------------------------------
 VFP ACL     1024     0         0           1024
 IFP ACL     4096     0         46          4050
 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

 Interface:
    GE3/0/25 to GE3/0/48
------------------------------------------------------------------------------
 Type       Total   Reserved  Configured  Remaining
------------------------------------------------------------------------------
 VFP ACL     1024     0         0           1024
 IFP ACL     4096     0         46          4050
 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
```

Table 1-1 Description on the fields of the **display acl resource** command

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, • IFP indicates the count of resources in the inbound direction, • EFP indicates the count of resources in the outbound direction • VFP indicates the count of resources that are before Layer 2 forwarding and applied in QinQ.
Total	Total number of ACLs supported
Reserved	Number of reserved ACLs
Configured	Number of configured ACLs

Field	Description
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 comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

all: All existing time ranges.

Description

Use the **display time-range** command to display the configuration and state of a specified or all time ranges.

A time range is active if the system time falls into its range, and if otherwise, inactive.

Examples

Display the configuration and state 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 1-2 Description on the fields of the **display time-range** command

Field	Description
Current time	Current system time
Time-range	The configuration and state of time range, such as time range name, its activated state, and start time and ending 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 comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

start-time: Start time of a periodic time range, in *hh*:*mm* format as 24-hour time, 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 as 24-hour time, 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, for this argument, 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 as 24-hour time, 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 from 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 from 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.

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.

Note that:

- 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.
- Up to 256 time ranges can be defined.

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 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-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: Defines a numbered access control list (ACL).

acl-number: IPv4 ACL number, in the range of 2000 to 4999.

- 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: Sets 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: 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 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 the name of the ACL.
- 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 it is empty.

Examples

Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Create IPv4 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

Enter the view of an IPv4 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Enter the view of an IPv4 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

Delete the IPv4 ACL with the number of 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

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 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

dest-acl-name: Name for the new 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 sequence number which is the smallest one among the available ones in the ACL range for the ACL type.

Description

Use the **acl copy** command to copy an existent IPv4 ACL (namely, the source IPv4 ACL) to generate a new one (namely, the destination IPv4 ACL). The new ACL is of the same type and has the same match order, match rules, rule numbering step and descriptions.

Note that:

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The generated ACL does not take the name of the source IPv4 ACL.

Examples

Copy basic IPv4 ACL 2008 to generate basic IPv4 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 create an IPv4 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the ACL description.

By default, no IPv4 ACL description is present.

Examples

Create a description for IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in eth 2/0/1
```

Create a description for IPv4 ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in eth 2/0/1
```

Create a description for ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in eth 2/0/1
```

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: 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 the specified or all IPv4 ACLs.

This command displays IPv4 ACL rules in the order in which the system compares a packet against them.

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 eth 2/0/1
```

Table 1-3 Description on the fields of the **display acl** command

Field	Description
Basic ACL 2001	The displayed information is about the 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 rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. This field appears as long as one match is found.
rule 5 comment This rule is used in eth 2/0/1	The description of ACL rule 5 is “This rule is used in eth 2/0/1.”

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: 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 about a specified or all IPv4 ACLs that are referenced by upper layer software.

Examples

Clear statistics about IPv4 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl counter 2001
```

Clear statistics about the IPv4 ACL named flow, which is referenced by upper layer software.

```
<Sysname> reset acl counter name flow
```

rule (in 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: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Specifies that the rule applies to only IP fragments. Note that a rule defined with the **fragment** keyword matches non-last IP fragments on an SA Series LPUs (line processing units) (for example, LSQ1FP48SA) or EA Series LPUs (for example, LSQ1GP12EA) while matching non-first IP fragments on an SC Series LPUs (for example, LSQ1GP24SC). For detailed information about types of LPUs, refer to the installation manual.

logging: Specifies to log matched packets.

source { *sour-addr sour-wildcard* | **any** }: Specifies a source address. The *sour-addr sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a 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 specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

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 the rule if it has existed.

Use the **undo rule** command to remove a basic IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not 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 greater

than the current highest rule ID. 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 may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Note

For a basic IPv4 ACL rule to be referenced by a QoS policy for traffic classification, the **logging** and **vpn-instance** keywords are not supported.

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 (in advanced IPv4 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [**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* [**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: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow 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), **udp** (17).

Table 1-4 Parameters for advanced IPv4 ACL rules

Parameters	Function	Description
source { sour-addr sour-wildcard | **any** }	Specifies a source address.	The sour-addr sour-wildcard argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a 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 specifies a destination IP address in dotted decimal notation. Setting the dest-wildcard to a 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 the rule to be reflective.	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and its statement can only be **permit**.
fragment	Specifies that the rule applies to only IP fragments.	A rule defined with the **fragment** keyword matches non-last IP fragments on an SA Series LPUs (for example, LSQ1FP48SA) or EA Series LPUs (for example, LSQ1GP12EA) while matching non-first IP fragments on an SC Series LPUs (for example, LSQ1GP24SC).

Parameters	Function	Description
time-range *time-range-name*	Specifies the time range in which the rule can take effect.	The time-range-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.
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.

If the *protocol* argument is set to **tcp** or **udp**, you may define the parameters in the following table.

Table 1-5 TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Defines a UDP or TCP source port against which UDP or TCP packets are matched.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), and **range** (inclusive range). *port1, port2*: TCP or UDP port number, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **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), or **www** (80). UDP port number can be represented in words as follows: **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), **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*]	Defines a UDP or TCP destination port against which UDP or TCP packets are matched.	

If the *protocol* argument is set to **icmp**, you may define the parameters in the following table.

Table 1-6 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. For available ICMP messages, see Table 1-7..

The following table provides the ICMP messages that you can specify in advanced IPv4 ACL rules.

Table 1-7 ICMP messages and their codes

ICMP message	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 define or modify an advanced IPv4 ACL rule. If the rule does not exist, it is created first.

Use the **undo rule** command to remove an advanced IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not 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 greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.

 **Note**

For an advanced IPv4 ACL to be referenced by a QoS policy for traffic classification:

- The **logging**, **reflective** and **vpn-instance** 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.

Examples

Define a rule to permit the TCP packets to pass with the destination port 80 sent from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] 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 (in 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: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

cos *vlan-pri:* Defines an 802.1p priority. The *vlan-pri* argument takes a value in the range 0 to 7; or its equivalent in words, **best-effort**, **background**, **spare**, **excellent-effort**, **controlled-load**, **video**, **voice**, or **network-management**.

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 frame encapsulation. The *lsap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code.

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 can take effect. The *time-range-name* argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

type *type-code type-wildcard:* Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating frame type. It is corresponding 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.

Description

Use the **rule** command to create an Ethernet frame header ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an Ethernet frame header ACL rule.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not 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 greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first 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.

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 create a rule description for an existing ACL rule or modify the rule description of an ACL rule 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, no rule description is created.

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 eth 2/0/1
```

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 eth 2/0/1
```

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 eth 2/0/1
```

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.

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

By default, 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: Defines a numbered IPv6 ACL.

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

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: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match. For how depth-first match works, refer to the “IPv6 ACL Match Order” section in accompanied *ACL Configuration*.
- **config**: Performs matching against rules in the order in which they are configured.

all: 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 or all IPv6 ACLs.

By default, the match order is **config**.

Note that:

- The match order setting is not available for simple IPv6 ACLs, because a simple IPv6 ACL can contain only one rule.
- 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 the name of the ACL.
- 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 it is empty.

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

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

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 sequence number which is the smallest one among the available ones in the ACL range for the ACL type.

Description

Use the **acl ipv6 copy** command to copy an existent IPv6 ACL (namely, the source IPv6 ACL) to generate a new one (namely, the destination IPv6 ACL), which is of the same type and has the same match order, match rules, rule numbering step and descriptions.

Note that:

- The source IPv6 ACL and the destination IPv6 ACL must be of the same type.
- The generated IPv6 ACL does not take the name of the source IPv4 ACL.

Examples

Copy IPv6 ACL 2008 to generate IPv6 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 create an IPv6 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the IPv6 ACL description.

By default, no IPv6 ACL description is present.

Examples

Create a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in eth 0
```

Create a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in eth 0
```

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: 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 specified or all IPv6 ACLs.

The output will be displayed in matching 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 eth 2/0/1
```

Table 1-8 Description on the fields of the **display acl ipv6** command

Field	Description
Basic IPv6 ACL 2001	The displayed information is about the 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 rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. The field appears as long as one match is found.
rule 0 comment This rule is used in eth 2/0/1	The description of ACL rule 5 is “This rule is used in eth 2/0/1.”

reset acl ipv6 counter

Syntax

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

View

User view

Default Level

2: System level

Parameters

all: All basic and advanced IPv6 ACLs.

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

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 about a specified or all IPv6 ACLs that are referenced by upper layer software.

Examples

Clear statistics about IPv6 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter 2001
```

Clear statistics about the IPv6 ACL named flow, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (in 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: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Specifies that the rule applies to only IP fragments.

logging: Specifies to log matched packets.

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 specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

Description

Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not 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 greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.
- You may use the **display acl ipv6** command to verify rules configured in an ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Note

For a basic IPv6 ACL to be referenced by a QoS policy for traffic classification, the **logging** and **fragment** keywords are not supported.

Examples

Create rules in IPv6 ACL 2000, to permit packets with source address being 2030:5060::9050/64 to pass.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
```

rule (in advanced IPv6 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [**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: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

protocol: Protocol carried on 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), **udp** (17).

Table 1-9 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.

Parameters	Function	Description
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	—
fragment	Specifies that the rule applies to only IP fragments.	—
time-range *time-range-name*	Specifies the time range in which the rule can take effect.	The time-range-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp,** you may define the parameters in the following table.

Table 1-10 TCP/UDP-specific match criteria for advanced IPv6 ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Defines the source port in the UDP/TCP packet.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments each specify a TCP or UDP port, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **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), or **www** (80). UDP port number can be represented in words as follows: **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), **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*]	Defines the destination port in the UDP/TCP packet.	

If the *protocol* argument is set to ICMPv6, you may define the parameters in the following table.

Table 1-11 ICMPv6-specific match criteria 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. For available ICMPv6 messages, see Table 1-12

The following table provides the ICMPv6 messages that you can specify in advanced IPv6 ACL rules.

Table 1-12 Available ICMPv6 messages

ICMPv6 message	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 IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Note that:

- You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.
- When defining ACL rules, you need not 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 greater than the current highest rule ID. 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 may use the **display acl ipv6** command to verify rules configured in an IPv6 ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

 **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.

Examples

Create a rule in IPv6 ACL 3000 to permit the TCP packets with the source address 2030:5060::9050/64 to pass.

```
<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 create a rule description for an existing ACL rule or modify the rule description of an ACL rule to, for example, describe the purpose of the ACL rule or its attributes.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, no rule description is created.

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 eth 2/0/1
```

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 eth 2/0/1
```

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: The step in which the rules in the IPv6 ACL is numbered, in the range 1 to 20.

Description

Use the **step** command to set a rule numbering step for the 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
```

System Volume Organization

Manual Version

20090615-C-1.01

Product Version

Release 6300 series

Organization

The System Volume is organized as follows:

Features	Description
Login	Upon logging into a device, you can configure user interface properties and manage the system conveniently. This document introduces the commands for: • Logging In Through the Console Port • Logging In Through Telnet/SSH • Logging In Using Modem • Specifying Source for Telnet Packets • Controlling Login Users
Basic System Configuration	Basic system configuration involves the configuration of device name, system clock, welcome message, and user privilege levels. This document introduces the commands for: • Configuring the device name, the system clock and a Banner • Configuring CLI Hotkeys • Configuring User Privilege Levels and Command Levels • Multiple-screen output configuring

Features	Description
Device Management	Through the device management function, you can view the current condition of your device and configure running parameters. This document introduces the commands for: • Rebooting a device • Configuring the scheduled automatic execution function • Specifying a file for the next device boot • Upgrading Boot ROM • Configuring a detection interval • Configuring temperature alarm thresholds for a board • Clearing the 16-bit interface indexes not used in the current system • Configuring the system load sharing function • Enabling Active/Standby Mode for Service Ports on SRPUs • Configuring the traffic forwarding mode of SRPUs • Configuring the working mode of EA LPUs • Enabling the port down function globally • Enabling expansion memory data recovery function on a board • Identifying and diagnosing pluggable transceivers
File System Management	A major function of the file system is to manage storage devices, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file. This document introduces the commands for: • File system management • Configuration File Management • FTP configuration • TFTP configuration
SNMP	Simple network management protocol (SNMP) offers a framework to monitor network devices through TCP/IP protocol suite. This document introduces the commands for: • Basic SNMP function configuration • SNMP log configuration • Trap configuration • MIB style configuration
RMON	RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. This document introduces the commands for RMON configuration (event group, history group, alarm group, private alarm group)
MAC Address Table Management	A switch maintains a MAC address table for fast forwarding packets. This document introduces the commands for: • How a MAC Address Table Entry is Generated • Configuring MAC Address Entries • Disabling MAC Address Learning • Configuring the Aging Timer for Dynamic MAC Address Entries • Configuring the MAC Learning Limit
System Maintaining and Debugging	For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors. This document introduces the commands for maintenance and debugging configuration

Features	Description
Information Center	As the system information hub, Information Center classifies and manages all types of system information. This document introduces the commands for: • Setting to Output System Information to the Console • Setting to Output System Information to a Monitor Terminal • Setting to Output System Information to a Log Host • Setting to Output System Information to the Trap Buffer • Setting to Output System Information to the Log Buffer • Setting to Output System Information to the SNMP Module • Setting to Save System Information to a Log File • Configuring Synchronous Information Output
PoE	The Power over Ethernet (PoE) feature enables the power sourcing equipment (PSE) to feed powered devices (PDs) from Ethernet ports through twisted pair cables. This document introduces the commands for: • Configuring PoE power supply • Configuring the PSE • Configuring the PoE interface • Configuring PoE power management • Configuring the PoE monitoring function • Online upgrading the PSE processing software • Enabling the PSE to detect nonstandard PDs
Track	The track module is used to implement collaboration between different modules through established collaboration objects. The detection modules trigger the application modules to perform certain operations through the track module. This document introduces the commands for: • Configuring Collaboration Between the Track Module and the Detection Modules • Configuring Collaboration Between the Track Module and the Application Modules
NQA	NQA analyzes network performance, services and service quality by sending test packets to provide you with network performance and service quality parameters. This document introduces the commands for: • Configuring the NQA Server • Enabling the NQA Client • Creating an NQA Test Group • Configuring an NQA Test Group • Configuring the Collaboration Function • Configuring Trap Delivery • Configuring Optional Parameters Common to an NQA Test Group • Scheduling an NQA Test Group
NTP	Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network. This document introduces the commands for: • Configuring the Operation Modes of NTP • Configuring the Local Clock as a Reference Source • Configuring Optional Parameters of NTP • Configuring Access-Control Rights • Configuring NTP Authentication

Features	Description
VRRP	Virtual Router Redundancy Protocol (VRRP) combines a group of switches (including a master and multiple backups) on a LAN into a virtual router called VRRP group. VRRP streamlines host configuration while providing high reliability. This document introduces the commands for: • IPv4-Based VRRP configuration • IPv6-Based VRRP configuration
HA	High Availability (HA) is to achieve a high availability of the system. Devices supporting HA are typically equipped with two SRPUs to provide active-standby backup. This document introduces the commands for: • Restarting the SMB • Manually Configuring Switchover Between the AMB and SMB
Hotfix	Hotfix is a fast, cost-effective method to fix software defects of the device without interrupting the running services. This document introduces the commands for hotfix operations (including loading, activating, running, deactivating, and deleting patch files)

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** [**command-authorization**] }

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.

command-authorization: Performs command authorization on TACACS authentication server.

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.
- If this command is executed with the **command-authorization** keywords specified, authorization is performed on the TACACS server whenever you attempt to execute a command, and the command can be executed only when you pass the authorization. Normally, a TACACS server contains a list of the commands available to different users.

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, whereas modem users and Telnet users are 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.

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 S7900E Series Ethernet Switches 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    9600       -      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

Filed	Description
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.

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

3Com S7900E Series Ethernet Switches 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:
<Sysname>
```

modem

Syntax

modem [**both | call-in** | **call-out**]

undo modem [**both** | **call-in** | **call-out**]

View

AUX interface view

Default Level

2: System level

Parameters

both: Allows both incoming and outgoing calls.

call-in: Allows incoming calls only.

call-out: Allows outgoing calls only.

Description

Use the **modem** command to enable the switch-side modem to accept incoming calls, initiate outgoing calls, or both.

Use the **undo modem** command to remove the modem dial-up configuration.

By default, modem calls are not allowed.

Examples

Enable the modem to accept both incoming and outgoing calls.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem both
```

modem auto-answer

Syntax

modem auto-answer

undo modem auto-answer

View

AUX interface view

Default Level

2: System level

Parameters

None

Description

Use the **modem auto-answer** command to configure the switch-side modem to operate in the auto-answer mode.

Use the **undo modem auto-answer** command to restore the default.

By default, the switch-side modem operates in the manual answer mode.

Examples

Configure the switch-side modem to operate in the auto-answer mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem auto-answer
```

modem timer answer

Syntax

modem timer answer *seconds*

undo modem timer answer

View

AUX interface view

Default Level

2: System level

Parameters

seconds: Timeout time in seconds, ranging from 1 to 60. The default is 30 seconds.

Description

Use the **modem timer answer** command to set the maximum amount of time that the modem waits for the carrier signal after the off-hook action during incoming call connection setup.

Use the **undo modem timer answer** command to restore the default.

Examples

Set the maximum amount of time that the switch-side modem waits for the carrier signal after the off-hook action to 45 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem timer answer 45
```

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 S7900E series Ethernet switches 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 0; 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 5.

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>
```

service-type

Syntax

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* }

View

Local user view

Default Level

2: System level

Parameters

ftp: Specifies the users to be of FTP type.

lan-access: Specifies the users to be of LAN-access type, which normally means Ethernet users, such as 802.1x users.

ssh: Specifies the users to be of SSH type.

telnet: Specifies the users to be of Telnet type.

terminal: Makes terminal services available to users logging in through the Console port.

level *level*: Specifies the user level for Telnet users, Terminal users, or SSH users. The *level* argument ranges from 0 to 3 and defaults to 0.

Description

Use the **service-type** command to specify the login type and the corresponding available command level.

Use the **undo service-type** command to cancel login type configuration.

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 commands of level 0 are available to the users logging in using the user name of **zbr**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user zbr
[Sysname-luser-zbr] service-type telnet level 0
```

To verify the above configuration, you can quit the system, log in again using the user name of **zbr**, and then list the available commands, as listed in the following.

```
[Sysname] quit
<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
```

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, modem users and 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 9,600.

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 stopbits cannot be 1.5 on an S7900E series Ethernet switch.

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
```

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.

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:
  display  Display current system information
  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
```

Table of Contents

1 Basic Configuration Commands

Basic Configuration Commands

clock datetime

Syntax

clock datetime *time date*

View

User view

Default Level

3: Manage level

Parameters

time: 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: 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 to universal time coordinated (UTC) time.

minus: Negative to UTC time.

zone-offset: Offset to the 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-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 section “Configuring User Privilege Levels and Command Levels” in the operation 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 ethernet 2/0/1, 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 ethernet command, and then return to user view.

Examples

Set the command level of the **interface** command to 0 in system view.

```
<Sysname> system-view
[Sysname] command-privilege level 0 view system interface
```

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-----------------
        telnet server enable
```

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 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:

- isis: Displays the isis configuration.
- isp: Displays the ISP configuration.
- post-system: Displays the post-system 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 of VLAN-interface 1 of the current device (the output information depends on the device model and the current configuration).

```
<Sysname> display current-configuration interface vlan-interface 1
#
interface Vlan-interface1
 ip address 192.168.0.72 255.255.255.0
 igmp group-policy 2000
 igmp static-group 224.1.1.1 source 1.1.1.1
 multicast boundary 224.5.5.0 24
 multicast boundary 224.1.1.0 24
 ntp-service multicast-server
 ntp-service multicast-server 224.0.1.0
 ntp-service multicast-server 224.0.1.2
#
return
```

Display the configuration from the line containing “user-interface” to the last line in the current validated configuration (the output information depends on the device model and 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 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 *User Interface 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 execute the command in any VLAN view, the command displays configuration of all the 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 the valid configuration information on interface Ethernet 2/0/1 (the output information depends on the current configuration of the device).

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
```

```
 port link-type hybrid
 port hybrid vlan 1 tagged
 port hybrid pvid vlan 3
#
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 main control board and interface boards.

Examples

Display system version information (The system version information varies with devices.).

```
<Sysname> display version
3Com Comware Platform Software
Comware Software, Version 5.20, Release 0000
Copyright (c) 2004-2008 Hangzhou 3Com Tech. Co., Ltd. All rights reserved.
3Com S7903E uptime is 0 week, 0 day, 7 hours, 34 minutes

MPU(M) 0:
Uptime is 0 weeks,0 days,7 hours,34 minutes
3Com S7903E MPU(M) with 1 BCM1125H Processor
DRAM:               512M bytes
FLASH:              64M bytes
NVRAM:              512K bytes
PCB 1 Version:      VER.B
PCB 2 Version:      VER.B
Bootrom Version:    206
CPLD 1 Version:     002
CPLD 2 Version:     002
Release Version:    3Com S7903E-0000
Patch Version  :    None
```

```
Slot 1 Without Board
LPU 2:
Uptime is 0 weeks,0 days,7 hours,32 minutes
3Com S7903E LPU with 1 BCM1122H Processor
DRAM:               256M bytes
FLASH:              0M bytes
NVRAM:              0K bytes
PCB 1 Version:      VER.A
PCB 2 Version:      VER.A
Bootrom Version:    201
CPLD 1 Version:     001
CPLD 2 Version:     001
Release Version:    3Com S7903E-0000
Patch Version  :    None
LPU 3:
Uptime is 0 weeks,0 days,7 hours,32 minutes
3Com S7903E LPU with 1 BCM1122H Processor
DRAM:               256M bytes
FLASH:              0M bytes
NVRAM:              0K bytes
PCB 1 Version:      VER.C
Bootrom Version:    205
CPLD 1 Version:     004
Release Version:    3Com S7903E-0000
Patch Version  :    None

Slot 4 Without Board
```

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 %
Input banner text, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Input banner text, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Input banner text, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Input banner text, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Input banner text, 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 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 exit the device.

Examples

Switch from Ethernet 2/0/1 interface view to system view, and then to user view.

```
[Sysname-Ethernet2/0/1] 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, as you do with the hot key **Ctrl+Z**.

Related commands: **quit**.

Examples

Return to user view from Ethernet2/0/1 view.

```
[Sysname-Ethernet2/0/1] 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 *User Interface 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.

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 3Com.

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 **R2000**.

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

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]
```

Table of Contents

1 Device Management Commands

Note

File names in this document comply with the following rules:

- Path + file name (namely, a full file name): File on a specified path. A full file name consists of 1 to 135 characters.
- “File name” (namely, only a file name without a path): File on the current working path. The file name without a path consists of 1 to 91 characters.

Device Management Commands

boot-loader

Syntax

boot-loader file *file-url* **slot** *slot-number* { **main** | **backup** }

View

User view

Default Level

2: System level

Parameters

file *file-url*: Specifies a file name, a string of 1 to 64 characters.

slot *slot-number*: Specifies the slot number of a board. The value range varies with devices.

main: Specifies a file as a main boot file.

backup: Specifies a file as a backup boot file.

Description

Use the **boot-loader** command to specify a boot file for the next boot.

A main boot file is used to boot a device and a backup boot file is used to boot a device only when a main boot file is unavailable.

Related commands: **display boot-loader**.

Examples

Specify the main boot file for the next boot of the active SRPU as **plat.app**.

```
<Sysname> boot-loader file plat.app slot 0 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!
```

Specify the main boot file for the next boot of the standby SRPU as **plat2.app**.

```
<Sysname> boot-loader file slot1#flash:/plat2.app 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!
```

bootrom

Syntax

bootrom { **backup** | **read** | **restore** | **update file** *file-url* } **slot** *slot-number-list* [**all** | **part**]

View

User view

Default Level

2: System level

Parameters

read: Reads Boot ROM, that is, copies the Boot ROM program form the normal partition of the Boot ROM memory to the flash as the backup, which will be used to restore the Boot ROM when the Boot ROM memory is broken.

restore: Restores Boot ROM, that is, restores the Boot ROM codes from the backup partition to the normal partition of the Boot ROM memory. When the current Boot ROM is broken, and you have backed up the codes, you can restore the Boot ROM by performing the restore operation.

backup: Backs up Boot ROM, that is, backs up the Boot ROM codes in the normal partition to the backup partition of the Boot ROM memory. When the current Boot ROM is broken, you can restore the Boot ROM program from the backup partition. You are recommended to back up the Boot ROM before upgrading it.

update file *file-url*: Upgrades Boot ROM, *where file-url* represents name of the file to be upgraded.

slot *slot-number-list*: Specifies a list of slot numbers of boards, in the format of { *slot-number* [**to** *slot-number*] }&<1-7>. The *slot-number* argument represents the slot number of a board and the value range varies with devices. &<1-7> indicates that you can specify up to seven lists of slot numbers.

all: Operates all contents of Boot ROM.

part: Operates only the extension part of Boot ROM (Boot ROM includes the basic part and the extension part, the basic part provides the basic operation items and the extension part provides more Boot ROM operation items).

Description

Use the **bootrom** command to read, restore, back up, or upgrade the Boot ROM program on a board(s).

If the arguments **all** and **part** are not specified, all contents of the Boot ROM program are operated.

Examples

Use the **mpu108.app** file to upgrade the Boot ROM program on the board in slot 1.

```
<Sysname> bootrom update file mpu108.app slot 1
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  Now updating bootrom, please wait...

  Start accessing bootflash chip...
  Bootrom update succeed in slot 1.
```

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 the specified board, where *slot-number* represents the slot number of a board. The value range varies with devices.

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 (The prompt information of this command varies with devices).

```
<Sysname> display boot-loader
  The primary app to boot of board 1 at this time is: flash:/ Switch.app
  The primary app to boot of board 1 at next time is: flash:/ Switch.app
  The slave app to boot of board 1 at next time is: flash:/Back.app
```

display cpu-usage

Syntax

display cpu-usage [**task**] [**slot** *slot-number*]

display cpu-usage *number* [*offset*] [**verbose**] [**slot** *slot-number*] [**from-device**]

View

Any view

Default Level

1: Monitor level

Parameters

number: Number of CPU usage statistics records to be displayed.

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.

verbose: Specifies to display detailed information of CPU usage statistics.

from-device: Displays external storage devices such as Flash and hard disk. The device currently does not support the **from-device** keyword.

task: Displays CPU usage of each task.

slot *slot-number*: Specifies to display the statistics of the CPU usage of a board. *slot-number* specifies the slot number of a board. The value range varies with devices.

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. The maximum number of records that can be saved depends on the device model. **display cpu-usage** *number* indicates the system displays *number* records from the newest (last) record. **display cpu-usage** *number offset* indicates the system displays *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:
     14% in last 5 seconds
     12% in last 1 minute
      8% in last 5 minutes
```

Display detailed information of the last CPU usage statistics record of the current tasks.

```
<Sysname> display cpu-usage task
===== Current CPU usage info =====
CPU Usage Stat. Cycle: 41 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2006-07-10  11:02:20
CPU Usage Stat. Tick : 0x1da0(CPU Tick High) 0x62a5077f(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x3d5b5ad1(CPU Tick Low)

TaskName        CPU        Runtime(CPU Tick High/CPU Tick Low)
b2X0             0%               0/   ce77f
VIDL            97%               0/3bc6e650
TICK             0%               0/  23ec62
STMR             0%               0/    ad24
DrTF             0%               0/   28b6b
DrTm             0%               0/   18a28
bCN0             0%               0/   d840e
```

```
…omitted…
```

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 1-1 display cpu-usage command output description

Field	Description
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 period in seconds
CPU Usage	CPU usage in percentage
CPU Usage Stat. Time	CPU usage statistics time in seconds
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 period 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.
TaskName	Task name
CPU	CPU usage of the current task
Runtime(CPU Tick High/CPU Tick Low)	Running time of the current task

display cpu-usage history

Syntax

display cpu-usage history [**task** *task-id*] [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

task *task-id*: Displays the CPU usage statistics of a task, where *task-id* represents the task number.

slot *slot-number*: Displays the statistics of the CPU usage of a board. *slot-number* specifies the slot number of a board and the value range varies with devices.

Description

Use the **display cpu-usage history** command to display the history statistics of the CPU usage in a chart. If no argument is specified, the CPU usage of the active main board is displayed.

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 last 60 CPU usage statistics records. 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(STMR)
```

The above output information indicates the CPU usage of task 6 (with the task name **STMR**) in the last 60 minutes: 5% in the twentieth minute, and 2% or lower than 2% at other times.

display device

Syntax

display device [**cf-card**] [[**shelf** *shelf-number*] [**frame** *frame-number*] [**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**]

View

Any view

Default Level

2: System level

Parameters

cf-card: Displays information of a compact Flash (CF).

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 range varies with devices.

frame *frame-number*: Displays detailed information of the specified frame. The *frame-number* argument represents a frame number and the value range varies with devices.

slot *slot-number*: Displays detailed information of the specified board. The *slot-number* argument represents the slot number of a board and the value range varies with devices.

subslot *subslot-number*: Displays detailed information of the specified subboard. The *subslot-number* represents the subslot of a subboard and the value range varies with devices.

verbose: Displays detailed information.

Description

Use the **display device** command to display information about storage media such as board, subboard, and CF card.

Examples

Display brief information of boards on a swtich. (The displayed information varies with devices.)

```
<Sysname> display device
Slot No.  Brd Type    Brd Status     Subslot Num     Sft Ver         Patch Ver
 0        NONE         Absent       0              NONE           None
 1        LSQ1MPUA     Master       0              S7900E-0000    None
 2        LSQ1FV48SA   Normal       0              S7900E-0000    None
 3        LSQ1PT4PSC   Normal       1              S7900E-0000    None
```

Table 1-2 display device command output description

Field	Description
Brd Type	Hardware type of a board
Brd Status	Board status
Sft Ver	Software version
Patch Ver	Patch Version

display device manuinfo

Syntax

display device manuinfo [**frame** *frame-number*] [**slot** *slot-number* [**subslot** *subslot-number*]]

View

Any view

Default Level

3: Manage level

Parameters

slot *slot-number*: Displays electrical label information of the specified board. The *slot-number* argument represents the slot number of a board and the value range varies with devices.

subslot *subslot-number*: Displays electrical label information of the specified subboard. The *subslot-number* represents the subslot of a subboard and the value range varies with devices.

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 device of a board during debugging or test of a board or 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 of slot 3.

```
<Sysname> display device manuinfo slot 3
DEVICE_NAME          : LSQ1PT4PSC
DEVICE_SERIAL_NUMBER : 03A43E1111111111
MAC_ADDRESS          : No
MANUFACTURING_DATE   : 2007-11-4
VENDOR_NAME          : 3Com
```

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):
-----------------------------------------------------
 Board    Temperature         Lower limit      Upper limit
 1        43                  20               70
 2        50                  0                80
 3        56                  0                80
```

display fan

Syntax

display fan [*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. The value varies with 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
 Fan  1 State: Normal
```

The above information displays all fans work normally.

display memory

Syntax

display memory [**slot** *slot-number*] [**cpu** *cpu-id*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Specifies the slot number of a board. The value range varies with devices.

cpu *cpu-id:* Display the memory of a specified CPU, where *cpu-id* represents the ID of the CPU. Support for the *cpu-id* argument depends on the device model.

Description

Use the **display memory** command to display the usage of the memory of all or specified boards of a device.

Examples

Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 395165344
Total Used Memory(bytes): 80815056
Used Rate: 20%
```

Table 1-3 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 [*power-id*]

View

Any view

Default Level

1: Monitor level

Parameters

power-id: Displays the status of the specified power supply unit, where *power-id* represents the power supply unit number. The value varies with devices.

Description

Use the **display power** to display the status of the power supply of a device.

Examples

Display the status of the power supply of a device (The displayed information varies with devices).

```
<Sysname> display power
 Power   1 State: Absent
 Power   2 State: Normal
```

The above information indicates that power supply 2 works normally, and power supply 1 and power supply 3 are 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 switch-mode status

Syntax

display switch-mode status

View

Any view

Default Level

0: Visit level

Parameters

None

Description

Use the **display switch-mode status** command to view the current traffic forwarding mode or working mode of all cards on the switch.

Examples

View the current traffic forwarding mode or working mode of all cards on the switch.

```
<Sysname> display switch-mode status
 Slot No.     Switch-Mode
    0         STANDARD-ROUTING
    2         ROUTING
    3         NONE
```

Table 1-4 display switch-mode status command output description

Field	Description
Slot No.	Card slot number
Switch-Mode	Traffic forwarding mode or working mode of a card
STANDARD-ROUTING	Standard forwarding mode with the route extension function
ROUTING	Route extension mode
NONE	This card is not an EA LPU.

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 1-5 shows the alarm information that may occur for the four types of commonly used transceivers.

Table 1-5 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.
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.

Field	Remarks
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.
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

Field	Remarks
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.

Note

For the pluggable transceivers supported by the S7900E series Ethernet switches, refer to *3Com S7900E Family Getting Started Guide*.

Examples

Display the alarm information of the pluggable transceiver plugged in interface GigabitEthernet 2/0/1.

```
<Sysname> display transceiver alarm interface gigabitethernet 2/0/1
GigabitEthernet2/0/1 transceiver current alarm information:
  RX loss of signal
  RX power low
```

Table 1-6 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.

Field	Description
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 H3C 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 H3C 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 H3C customized anti-spoofing pluggable optical transceivers.

Examples

Display the currently measured value of the digital diagnosis parameters of the H3C customized anti-spoofing pluggable optical transceiver plugged in interface GigabitEthernet 2/0/2.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 2/0/2
GigabitEthernet2/0/2 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 1-7 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.

Field	Description
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 GigabitEthernet 2/0/3.

```
<Sysname> display transceiver interface gigabitethernet 2/0/3
GigabitEthernet2/0/3 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                   : H3C
  Ordering Name                 : SFP-GE-SX-MM850
```

Table 1-8 display transceiver command output description

Field	Description
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.

Field	Description
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: • H3C customized anti-spoofing transceiver: **H3C** 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 H3C 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 H3C 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 H3C customized anti-spoofing pluggable transceivers.

Examples

Display the electrical label information of the H3C customized anti-spoofing pluggable transceiver plugged in interface GigabitEthernet 2/0/4.

```
<Sysname> display transceiver manuinfo interface gigabitethernet 2/0/4
GigabitEthernet2/0/4 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2006-09-01
  Vendor Name          : H3C
```

Table 1-9 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 vendor who customizes the transceiver, that is, H3C.

loadsharing enable

Syntax

loadsharing enable

undo loadsharing enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **loadsharing enable** command to enable the load sharing function of the system.

Use the **undo loadsharing enable** command to disable the load sharing function of the system.

By default, the system load sharing function is disabled.

- When the system load sharing function is enabled, the active SRPU and the standby SRPU share the traffic that needs inter-board forwarding.
- When the system load sharing function is disabled, only the active SRPU forwards the traffic that needs inter-board forwarding.

Note

- Load sharing is applicable to unicast traffic only.
- The S7902E switches are designed to work in the load sharing mode, and do not support the command.

Examples

Enable the load sharing function of the system.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] loadsharing enable
```

monitor handshake-timeout disable-port

Syntax

monitor handshake-timeout disable-port

undo monitor handshake-timeout disable-port

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **monitor handshake-timeout disable-port** command to enable the port down function globally. With this function enabled, if the SRPU is plugged out or reboots abnormally, all service ports will be down immediately.

Use the **undo monitor handshake-timeout disable-port** command to disable the function.

By default, the port down function is disabled.

Examples

Enable the port down function globally

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] monitor handshake-timeout disable-port
Open port-down function in slot 1 !
Open port-down function in slot 2 !
Open port-down function in slot 3 !
```

mmu-monitor enable

Syntax

mmu-monitor enable *slot-number*

undo mmu-monitor enable *slot-number*

View

System view

Default Level

2: System level

Parameters

slot-number: Slot number of a board. The value range varies with devices.

Description

Use the **mmu-monitor enable** command to enable expansion memory data recovery function on a board. After this function is enabled, data monitoring of the expansion memory on the specified EA LPU or LSQ1SRP1CB SRPU is performed. When data error occurs, data recovery will start automatically.

Use the **undo mmu-monitor enable** command to disable the function.

By default, data recovery function of the expansion memory is enabled.

Examples

Disable the expansion memory data recovery function on the EA LPU in slot 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] undo mmu-monitor enable 1
```

reboot

Syntax

reboot [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot-number*: Specifies the slot number of a board. The value range varies with devices.

Description

Use the **reboot** command to reboot a board, or the whole system.

Caution

- If you do not specify the **slot** keyword, or reboot the active main board, the execution of the **reboot** command results in the reboot of the whole device.
- Device reboot may result in the interruption of the ongoing services. Be careful to use these commands.
- If a main boot file fails or does not exist, the device cannot be rebooted with this 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
Starting......
```

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
Starting......
```

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 system.

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.
- This feature does not support the active main board (AMB) and standby main board (SMB) switchover function. That is, after this feature is configured on the AMB, the configuration is not backed up to the SMB.

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 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/5/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 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/5/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
```

strict-standby enable

Syntax

strict-standby enable

undo strict-standby enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **strict-standby enable** command to enable active/standby mode for service ports on SRPUs.

Use the **undo strict-standby enable** command to disable active/standby mode for service ports on SRPUs.

Note

The active/standby mode of service ports is only applicable when the S7903E, S7906E, S7906E-V, or S7910E switch uses LSQ1SRP2XB or LSQ1SRP12GB to operate in dual-SRPU mode.

Examples

Enable active/standby mode for service ports on SRPUs.

```
<Sysname> system-view
[Sysname] strict-standby enable
```

switch-mode (for SRPU)

Syntax

When the SRPU is LSQ1SRP1CB:

switch-mode { **l2-enhanced** | **standard-bridging** | **standard-routing** }

undo switch-mode

When the SRPU is LSQ1SRP2XB, LSQ1SRPB, or LSQ1MPUA:

switch-mode { **l2-enhanced** | **standard** }

undo switch-mode

View

System view

Default Level

2: System level

Parameters

l2-enhanced: Indicates the enhanced Layer 2 forwarding mode with the MAC extension function when the SRPU is LSQ1SRP1CB, and the enhanced Layer 2 forwarding mode when the SRPU is LSQ1SRP2XB, LSQ1SRPB, or LSQ1MPUA.

standard: Indicates the standard forwarding mode.

standard-bridging: Indicates the standard forwarding mode with the MAC extension function.

standard-routing: Indicates the standard forwarding mode with the route extension function.

Description

Use the **switch-mode** command to configure the traffic forwarding mode of an SRPU.

Use the **undo switch-mode** command to restore the default traffic forwarding mode of the SRPU.

- The default traffic forwarding mode of LSQ1SRP1CB is **standard-routing**.
- The default traffic forwarding mode of LSQ1SRP2XB, LSQ1SRPB, or LSQ1MPUA is **standard**.

Note

To make the configured forwarding mode take effect, you need to save the configuration and restart the switch.

Examples

Configure the traffic forwarding mode of the SRPU (LSQ1MPUA) as the enhanced Layer 2 forwarding mode.

```
<Sysname> system-view
[Sysname] switch-mode l2-enhanced
```

Restore the default traffic forwarding mode of the SRPU.

```
<Sysname> system-view
[Sysname] undo switch-mode
```

switch-mode (for LPU)

Syntax

switch-mode { **bridging** | **routing** } **slot** *slot-num*

undo switch-mode slot *slot-num*

View

System view

Default Level

2: System level

Parameters

bridging: Indicates the MAC extension mode.

routing: Indicates the route extension mode.

slot-num: Number of the slot where the LPU resides.

Description

Use the **switch-mode** command to configure the working mode of an EA LPU.

Use the **undo switch-mode** command to restore the default working mode of the EA LPU.

By default, the working mode of an EA LPU is determined by the SRPU model and the current traffic forwarding mode of the SRPU. Refer to Table 1-10 for details.

Table 1-10 Default working mode of EA LPUs

nSRPU model	Current traffic forwarding mode of the SRPU	Default working mode of EA LPUs
LSQ1SRP2XB, LSQ1SRPB, LSQ1MPUA	**l2-enhanced** or **standard**	**routing**

nSRPU model	Current traffic forwarding mode of the SRPU	Default working mode of EA LPUs
LSQ1SRP1CB	**l2-enhanced** or **standard-bridging**	**bridging**
	standard-routing	**routing**

Note

- When the SRPU of the S7900E switch is LSQ1SRP1CB, it is recommended not to modify the default working mode the EA LPUs.
- When the SRPU of the S7900E switch is LSQ1SRP2XB, LSQ1SRPB, or LSQ1MPUA, if an EA LPU is connected to a Layer 2 forwarding network with a large number of MAC addresses, you can configure the EA LPU to work in the MAC extension mode.
- To make the configured working mode take effect, you need to save the configuration and restart the switch.

Examples

Configure the working mode of the EA LPU on slot 2 of the S7902E switch as the MAC extension mode.

```
<Sysname> system-view
[Sysname] switch-mode bridging slot 2
```

Restore the default working mode of the EA LPU on slot 2 of the S7902E switch.

```
<Sysname> system-view
[Sysname] undo switch-mode slot 2
```

temperature-limit

Syntax

temperature-limit *slot-number lower-value upper-value*

undo temperature-limit *slot-number*

View

System view

Default Level

2: System level

Parameters

slot-number: Slot number.

lower-value: Lower temperature limit in Celsius degrees, in the range 0°C to 70°C (32°F to 158°F).

upper-value: Upper temperature limit in Celsius degrees, in the range 20°C to 90°C (68°F to 194°F).Description

Use the **temperature-limit** command to set the temperature alarm threshold on a board.

Use the **undo temperature-limit** command to restore the temperature alarm threshold to the default.

By default, the temperature alarm thresholds for a board are as follows:

- Upper limit: 80°C (176°F)
- Lower limit: 0°C (32°F)

Note

The *upper-value* argument must be bigger than the *lower-level* argument.

Examples

Set the lower temperature limit on board 1 to 10 Celsius degrees and the upper temperature limit to 75 Celsius degrees.

```
<Sysname> system-view
[Sysname] temperature-limit 1 10 75
Setting temperature limit succeeded.
```

Table of Contents

1 File System Management Commands

Note

Throughout this document, a filename can be entered as either of the following:

- A fully qualified filename with a path included to indicate a file under a specific path. The filename can be 1 to 135 characters in length, excluding the ending character.
- A short filename with no path to indicate a file in the current working path. The filename can be 1 to 91 characters in length, excluding the ending character.

File System Configuration Commands

cd

Syntax

cd *directory*

View

User view

Default Level

3: Manage level

Parameters

directory: Name of the target directory.

Description

Use the **cd** command to change the current working directory.

Examples

Change the current directory to Flash:.

```
<Sysname> cd flash:
```

Return to the upper directory (Remember to enter a space after the keyword **cd**).

```
<Sysname> cd ..
```

Return to the root directory.

```
<Sysname> cd /
```

After you change the current directory using the **cd** command, you can use the **pwd** command to view the path of the current working directory.

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.
```

Copy file **1.cfg** under the folder **test** to folder **testbackup**, and save it as **1backup.cfg**.

```
<Sysname> copy flash:/test/1.cfg cfa0:/testbackup/1backup.cfg
Copy flash:/test/1.cfg to flash:/testbackup/1backup.cfg?[Y/N]:y

%Copy file flash:/test/1.cfg to flash:/testbackup/1backup.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 device 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.

This command supports the wildcard *.

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.

```
<Sysname> delete tt.cfg
...
Delete flash:/tt.cfg?[Y/N]:y
.
%Delete file 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.

This command supports the wildcard *.

Examples

Display information about all files and folders.

```
<Sysname> dir /all
Directory of flash:/

   0   -rw-   6985954  Apr 26 2005 21:06:29   mainup.app
   1   -rwh      1842  Apr 27 2005 04:37:17   private-data.txt
   2   -rw-      1518  Apr 26 2005 12:05:38   config.cfg
   3   -rw-      2045  May 04 2005 15:50:01   backcfg.cfg
   4   -rwh       428  Apr 27 2005 16:41:21   hostkey
   5   -rwh       572  Apr 27 2005 16:41:31   serverkey
   6   -rw-   2737556  Oct 12 2005 01:31:44   [old.app]

64389 KB total (54880 KB free)
```

[ ] indicates this file is in the recycle bin.

Table 1-1 dir command output description

Field	Description
Directory of	Current directory
d	Directory. The item is a file if d is not displayed.
r	The file or directory is readable.
w	The file or directory is writeable.
h	The file or directory 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.

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 prevent undesirable consequents resulting from misoperations, the **alert** mode is preferred.

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 device name.

Description

Use the **fixdisk** command to restore the space of a storage device when it becomes unavailable because of some abnormal operation.

Note that, you can execute the **fixdisk** command for the storage device on the active main board (AMB), but you cannot execute the command for the storage device on the standby main board (SMB).

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* [**FAT16** | **FAT32**]

View

User view

Default Level

3: Manage level

Parameters

device: Name of a storage device (for example flash or cf).

FAT16: Formats a storage device using the FAT16 format. FAT16 does not support **Tab** matching but needs to be input completely if used, and is not applicable to a Flash card.

FAT32: Formats a storage device using the FAT32 format. FAT32 does not support **Tab** matching but needs to be input completely if used, and is not applicable to a Flash card.

Description

Use the **format** command to format a storage device.

Caution

Formatting a storage device results in loss of all the files on the storage device and these files cannot be restored. In particular, if there is a startup configuration file on a storage device, formatting the storage device 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 device.

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**.

```
<Sysname> mkdir test
....
%Created dir flash:/test
```

Create folder **test/subtest**.

```
<Sysname> mkdir test/subtest
....
%Created dir flash:/test/subtest
```

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 3Com.
```

Display the contents of file **testcfg.cfg**.

```
<Sysname> more testcfg.cfg

#
 version 5.20, Beta 1201, Standard
#
 sysname Sysname
#
vlan 2
#
return
<Sysname>
```

mount

Syntax

mount *device*

View

User view

Default Level

3: Manage level

Parameters

device: Name of a storage device.

Description

Use the **mount** command to mount a hot swappable storage device, such as a CF card, etc (excluding Flash). This command is effective only when the device is in unmounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the board when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a lower version system, the system may not be able to recognize the device automatically, and you need to use the **mount** command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device.

Related commands: **umount**.

Examples

Mount a CF card of the AMB.

```
<Sysname> mount cf:
% Mount cf: successfully.
%Apr 23 01:50:00:628 2003 Sysname VFS/4/LOG:
cf: mounted into slot 4.
```

Mount a CF card of the SMB (assume the SMB is in slot 5).

```
<Sysname> mount slot5#cf:

% Mount slot5#cf: successfully.
%Apr 23 01:50:00:628 2003 Sysname VFS/5/LOG:
cf: mounted into slot 5.
```

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.bak**.

```
<Sysname> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak?[Y/N]:y
...
%Renamed file flash:/sample.txt to flash:/sample.bak
```

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.

Unlike this command, the **delete** *file-url* command only moves a file to the recycle bin. To delete the file in the recycle bin, you need to execute the **reset recycle-bin** command in the original directory of the file.

Examples

There are three files **flash:/a.cfg**, **flash:/b.cfg**, and **flash:/test/c.cfg** in the recycle bin. Permanently delete file **flash:/a.cfg** and **flash:/b.cfg**.

- Display all the files in the recycle bin in directory **flash:**.

```
<Sysname> dir /all
Directory of flash:/

   0     -rwh      3080  Apr 26 2000 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2000 13:45:36   config.cfg
   2     -rw-   8036197  May 14 2000 10:13:18   main.app
   3     -rw-      2386  Apr 26 2000 13:30:30   back.cfg
   4     drw-         -  May 08 2000 09:49:25   test
   5     -rwh       716  Apr 24 2007 16:17:30   hostkey
   6     -rwh       572  Apr 24 2007 16:17:44   serverkey
   7     -rw-      2386  May 08 2000 11:14:20   [a.cfg]
   8     -rw-      3608  Dec 03 2007 17:29:30   [b.cfg]

64389 KB total (56514 KB free)
```

//The above information indicates that in directory **flash:**, there are two files **a.cfg** and **b.cfg** in the recycle bin.

- Delete the files in directory **flash:** that are already in the recycle bin.

```
<Sysname> reset recycle-bin
Clear flash:/~/a.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
....
%Cleared file flash:/~/a.cfg.
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 all the files in the recycle bin are deleted.

```
<Sysname> dir /all
Directory of flash:/

   0     -rwh      3080  Apr 26 2000 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2000 13:45:36   config.cfg
   2     -rw-   8036197  May 14 2000 10:13:18   main.app
   3     -rw-      2386  Apr 26 2000 13:30:30   back.cfg
   4     drw-         -  May 08 2000 09:49:25   test
   5     -rwh       716  Apr 24 2007 16:17:30   hostkey
```

```
   6     -rwh       572  Apr 24 2007 16:17:44   serverkey

64389 KB total (56518 KB free)
```

// The above information indicates that file **flash:/a.cfg** and **flash:/b.cfg** are deleted permanently.

- In directory **flash:/test**, see whether the file in the recycle bin is deleted or not.

```
<Sysname> cd test
<Sysname> dir /all
Directory of flash:/test/

   0     drw-         -  Dec 03 2007 18:19:09   subtest
   1     -rw-      2386  Dec 03 2007 18:43:41   [c.cfg]

64389 KB total (56518 KB free)
```

// The above information indicates that file **flash:/test/c.cfg** in directory **flash:/test** is not deleted and is still in the recycle bin.

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.
```

umount

Syntax

umount *device*

View

User view

Default Level

3: Manage level

Parameters

device: Name of a storage device.

Description

Use the **umount** command to unmount a hot swappable storage device, such as a CF card, excluding Flash. This command is effective only when the storage device is in mounted state.

By default, a storage device is in the mounted state. You need to unmount it before removing it from the device.

Note that:

- When mounting or unmounting a storage device, or performing file operations on it, do not unplug or switchover the storage device or the board where the storage device resides. Otherwise, the file system could be damaged.
- When a storage device is connected to a lower version system, the system may not be able to recognize the device automatically, and you need to use the **mount** command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device.

Related commands: **mount**.

Examples

Unmount a CF card of the AMB.

```
<Sysname> umount cf:
% Umount cf: successfully.
%Apr 23 01:49:20:929 2003 Sysname VFS/5/LOG:
cf: umounted from slot 0.
```

Unmount a CF card of the SMB (assume the SMB is in slot 5).

```
<Sysname> umount slot5#cf:
% Umount slot5#cf: successfully.
%Apr 23 01:49:20:929 2003 Sysname VFS/5/LOG:
cf: umounted from slot 5.
```

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> undel 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

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 backup the startup configuration file (used at the next system startup) using a filename you specify. If you do not specify this filename, the original filename is used. This command only backs up the startup configuration file of the AMB.

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:/config.cfg
  Next startup saved-configuration file:             flash:/test.cfg
<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 **test.cfg** to TFTP server 2.2.2.2, where the file is saved as **192-168-1-26.cfg**.

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 current configuration file saved on the storage medium of the device.

After the device is powered on, if you find that some configurations are not validated or incorrect, you may use this command to display the configuration used for the current startup. During device management and maintenance, you can also use this command to check whether important configurations are saved to the current configuration file.

If the device starts up without using the configuration file, meaning the displayed startup configuration file is NULL after you execute the **display startup** command, there will be no information displayed when you execute the **display saved-configuration** command; if you have saved the configuration to the configuration file after the device starts up, the information last saved in the configuration file is displayed.

Related commands: **save**, **reset saved-configuration**; **display current-configuration** in *Basic Configuration Commands* in the *System Volume*.

Examples

Display the currently running configuration file saved on the storage medium of the device.

```
<Sysname> display saved-configuration
#
 version 5.20, Test 5310
#
 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 currently running configuration file saved on the storage medium of the device with a number identifying each line.

```
<Sysname> display saved-configuration by-linenum
    1:  #
    2:   version 5.20, Test 5310
    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 file used at the current system startup and the configuration file to be used at the next system startup.

Note that:

- The SMB is started and runs based on the current configurations of the AMB; therefore the current startup configuration files displayed on the AMB and SMB are always the same.
- After a switchover between the AMB and SMB, the new AMB 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 AMB is displayed as NULL and that of the new SMB is also NULL to keep consistent with the new AMB.

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:          flash:/testcfg.cfg
  Next startup saved-configuration file:             flash:/testcfg.cfg
  Bootrom-access enable state:                       enabled
```

Table 1-2 display startup command output description

Field	Description
Current Startup saved-configuration file	The configuration file used for the current startup
Next startup saved-configuration file	The configuration file used for the next startup

reset saved-configuration

Syntax

reset saved-configuration

View

User view

Default Level

2: System level

Parameters

None

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 the device. Use it with caution.

Related commands: save, display saved-configuration.

Examples

Delete the currently running configuration file from the storage medium of the device.

```
<Sysname> reset saved-configuration
The saved configuration will be erased.
Are you sure? [Y/N]:y
Configuration in the device is being cleared.
Please wait .......
Configuration in the device is cleared.
```

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.

This command downloads the configuration file to the AMB and specifies the file as the configuration file to be used at the next startup of the AMB, and meanwhile copies the file to the SMB and specifies the file as the configuration file to be used at the next startup of the SMB.

If the file to be downloaded has the same filename as an existing file on the AMB or SMB, you will be prompted whether you want to overwrite the existing file or not. In addition, both the AMB and the SMB are assumed to use the storage devices of the same type when the device is checking the filename or backing up the configuration file to the SMB. When backing up the configuration file to the SMB, the device saves the file to the same directory on the SMB as on the AMB, that is, the root directory. If the AMB and SMB are of different types, for example, a Flash and a CF card respectively, the backup operation will fail.

Examples

Download configuration file **config.cfg** from the TFTP server whose IP address is 2.2.2.2, and the configuration file is to be used 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-name* | **safely**]

View

Any view

Default Level

2: System level

Parameters

file-name: File name, whose extension name must be .cfg.

safely: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

Description

Use the **save** *file-name* 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 *file-name* does not exist, the system will create the file and then save the configuration to the file.

Use the **save** [**safely**] command to save the current configuration to a configuration file and specify the file as the startup configuration file for the next system startup.

Note that:

If you use the **save** *file-name* command, even if the configuration file auto-save function is enabled, the SMB does not automatically save the current configuration to its own configuration file. If you do not specify the *file-name* argument, the SMB automatically saves the current configuration when the AMB executes the **save** [**safely**] command.

Related commands: reset saved-configuration, display current-configuration, display saved-configuration.

Examples

Save the current configuration file to the default directory.

```
<Sysname> save
The current configuration will be written to the device.
Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/testcfg.cfg](To leave the
existing filename unchanged, press the enter key):
flash:/testcfg.cfg exists, overwrite?[Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/testcfg.cfg. Please wait...
.
Configuration is saved to flash successfully.
<Sysname>
```

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. After the function is enabled, when you configure to save the current configuration on the AMB, the SMB automatically saves the current configuration to its configuration file.

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*

undo startup saved-configuration

View

User view

Default Level

2: System level

Parameters

cfgfile: Configuration file name.

Description

Use the **startup saved-configuration** command to specify a startup configuration file (the configuration file to be used at the next system startup).

Use the **undo startup saved-configuration** command to configure the system to start up with the null configuration, that is, the factory configuration.

The specified file must be ended with a .cfg extension and saved in the root directory of the storage device.

Related commands: **display startup**.

Examples

Specify a startup configuration file for the next system startup.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ....... Done!
```

2 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 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
```

The output indicates that the FTP server is running, and supports only one concurrent login user; now one logged-in user is present; FTP connection idle time is 30 minutes, and put method is **fast**.

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:
```

Table 2-1 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.

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 use ACLs to restrict that which FTP clients are allowed to access the device.

Use the **undo ftp server acl** command to restore the default.

By default, no restriction is configured.

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 2000
```

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.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.

Examples

Disable the FTP server.

```
<Sysname> system-view
[Sysname] undo ftp server
% Close FTP server
```

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. The default is 30 minutes.

Description

Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

After you log in to an FTP server, an FTP connection is established. When the connection is disrupted, the FTP server, if not notified, cannot realize that and thus maintains the connection. 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

- You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to ftp.
- The prompt information in this section is that in the network where the 3Com S7900E series Ethernet switches act as the FTP server. If you use other devices as the FTP server, PC for example, the prompt information may be different.

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.

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the file transfer mode is ASCII.

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).

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the transfer mode is ASCII mode.

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. If no connection is established between the device and the remote FTP server, the command exits to the user view directly.

Related commands: **close**, **disconnect**, **quit**.

Examples

Terminate the connection with the remote FTP server and return to user view.

```
[ftp] bye
221 Server closing.
```

cd

Syntax

cd *pathname*

View

FTP client view

Default Level

3: Manage level

Parameters

pathname: Path name.

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.

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**).

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 2-2 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, and the deleted file can never be restored.

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

The **ls** command can only display the names of files and directories, 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 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 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 Login OK
[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: File name on the remote FTP server.

localfile: Local file name.

Description

Use the **get** command to download a file from a remote FTP server and save it.

If no local file name is specified, the local file uses the name of the source file on the FTP server by default.

Examples

Download file **testcfg.cfg** and save it as **aa.cfg**.

```
[ftp]get testcfg.cfg aa.cfg
```

```
227 Entering Passive Mode (192,168,1,50,17,163).
125 ASCII mode data connection already open, transfer starting for /testcfg.cfg.
.....226 Transfer complete.
FTP: 5190 byte(s) received in 7.754 second(s), 669.00 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:/temp
```

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, whereas the **dir** command can display other related information of the files and directories, such as the size, and the date they are 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.app
arbasicbtm.app
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: Directory name.

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.

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: Local file name.

remotefile: Name of the file to be saved on the remote FTP server.

Description

Use the **put** command to upload a file 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.

Examples

Upload source file **cc.txt** to the remote FTP server and save it as **dd.txt**.

```
[ftp] put cc.txt dd.txt
227 Entering Passive Mode (192,168,1,50,17,169).
125 ASCII mode data connection already open, transfer starting for /dd.txt.
226 Transfer complete.
FTP: 9 byte(s) sent in 0.112 second(s), 80.00 byte(s)/sec.
```

pwd

Syntax

pwd

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **pwd** command to display the current working directory on the remote FTP server.

Examples

Display the current working directory on the remote FTP server.

```
[ftp] pwd
257 "/temp" is current directory.
```

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 2-3 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
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

Field	Description
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 verbose function to display detailed prompt information.

Use the **undo verbose** command to disable the verbose function.

By default, the verbose function is enabled.

Examples

Enable the verbose function.

```
[ftp] verbose
FTP: verbose is on
```

3 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 use ACLs to restrict access to the TFTP server

Use the **undo tftp-server acl** command to restore the default.

By default, no restriction is configured.

You can reference an ACL control TFTP server access.

For more information about ACL, refer to *ACL Configuration* in the *Security Volume.*

Examples

Reference ACL 2000 to control IPv4 TFTP server access.

```
<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
```

Reference IPv6 ACL 2001 to control Ipv6 TFTP server access.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2030:5060::9050/64
[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.

source-filename: Source file name.

destination-filename: Destination file name.

get: Downloads a file in normal mode.

put: Uploads a file.

sget: Downloads a file in secure mode.

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, the saved file uses the source file name.
- 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.
```

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.
```

Table of Contents

1 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 for all the current communities.

```
<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 1-1 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 1-2 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 1-1.

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 SNMP 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 1-3 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 1-4 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 an 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 1-5 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
   bgp trap enable
   configuration trap enable
   flash trap enable
   fr trap enable
   isdn trap enable
   mpls trap enable
   ospf trap enable
   standard trap enable
   system trap enable
   voice trap enable
   vrrp trap enable

   Enable traps: 11; 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 1-6 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 1-1for 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 Link up/down 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 2/0/1 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 2/0/1
[Sysname-GigabitEthernet2/0/1] 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.

mode: Specifies the encryption algorithm and authentication algorithm. The two encryption algorithms Advanced Encryption Standard (AES), 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 *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 NMS and 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 a specified SNMP logging is enabled, when NMS performs a specified operation on 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 number of bytes of an SNMP packet that can be received or sent by an agent, in the range 484 to 17,940. The default value is 1,500 bytes.

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 number of bytes that can be received or sent by an 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*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

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

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.

vpn-instance *vpn-instance-name*: Specifies the VPN where the target host resides, where *vpn-instance-name* indicates the VPN instance name and is a string of 1 to 31 characters. It is case sensitive and is applicable only in a network supporting IPv4. If you execute the command with this keyword and argument combination, you need to add the agent into this VPN domain, and ensure that the route between the agent and the NMS is available.

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. The number of target hosts that can be configured varies with the device model.

- 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
```

Enable the device to send SNMP traps to the device which is in VPN 1 and has an IP address of 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 vpn-instance vpn1 params
securityname public
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [**bgp** | **configuration** | **flash** | **mpls** | **ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] * | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

undo snmp-agent trap enable [**bgp** | **configuration** | **flash** | **mpls** | **ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] * | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

View

System view

Default Level

3: Manage level

Parameters

bgp: Enables the sending of traps of the BGP module.

configuration: Enables the sending of configuration traps.

flash: Enables the sending of FLASH-related traps.

mpls: Enables the sending of traps of the MPLS module.

ospf: Enables the sending of traps of the OSPF module.

- *process-id*: OSPF process ID, in the range 1 to 65535.
- **ifauthfail**: Traps for interface authentication failure.
- **ifcfgerror**: Traps for interface configuration error.
- **ifrxbadpkt**: Traps for receiving incorrect packets.
- **ifstatechange**: Traps for interface state change.
- **iftxretransmit**: Traps for the interface to receive and forward packets.
- **lsdbapproachoverflow**: Traps for LSDB to be overflowed.
- **lsdboverflow**: Traps for LSDB overflow.
- **maxagelsa**: Traps for LSA max age.
- **nbrstatechange**: Traps for neighbor state change.
- **originatelsa**: Traps for local LSA generation.
- **vifcfgerror**: Traps for virtual interface configuration error.
- **virifauthfail**: Traps for virtual interface authentication failure.
- **virifrxbadpkt**: Traps for virtual interface receiving error packets.
- **virifstatechange**: Traps for virtual interface state changes.
- **viriftxretransmit**: Traps for virtual interface receiving and forwarding packets.
- **virnbrstatechange**: Traps for neighbor state change of the virtual interface.

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 System (a private MIB) traps.

vrrp: Traps of the VRRP module.

- **authfailure**: Traps for VRRP authentication failure.
- **newmaster**: Enables the sending of VRRP newmaster traps when the device becomes the master.

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 is enabled globally.

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 Ethernet1/1, 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 Ethernet1/1, 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** { **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, 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.

- **des56**: Specifies the privacy protocol to be data encryption standard (DES).
- **aes128**: Specifies the privacy protocol to be advanced encryption standard (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 **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

Table of Contents

1 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 1-1 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 1-2 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. If no entry number is specified, the log information for all event entries is displayed.

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 1-3 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 2/0/1.

```
<Sysname> display rmon history GigabitEthernet 2/0/1
HistoryControlEntry 1 owned by null is VALID
  Samples interface     : GigabitEthernet2/0/1<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 1-4 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.

Field	Description
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.
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 (Support for the field depends on the device model.), 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.GigabitEthernet2/0/1
  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 1-5 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.
Variable formula	Variable formula
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 2/0/1.

```
<Sysname> display rmon statistics GigabitEthernet 2/0/1
EtherStatsEntry 1 owned by null is VALID.
  Interface : GigabitEthernet2/0/1<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 1-6 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 by the interface during the statistical period, corresponding to the MIB node etherStatsOctets.

Field	Description
etherStatsPkts	Number of packets received by the interface during the statistical period, corresponding to the MIB node etherStatsPkts.
etherStatsBroadcastPkts	Number of broadcast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsBroadcastPkts.
etherStatsMulticastPkts	Number of multicast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsMulticastPkts.
etherStatsUndersizePkts	Number of undersize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsUndersizePkts.
etherStatsOversizePkts	Number of oversize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsOversizePkts.
etherStatsFragments	Number of undersize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsFragments.
etherStatsJabbers	Number of oversize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsJabbers.
etherStatsCRCAlignErrors	Number of packets with CRC errors received on the interface during the statistical period, corresponding to the MIB node etherStatsCRCAlignErrors.
etherStatsCollisions	Number of collisions received on the interface during the statistical period, corresponding to the MIB node etherStatsCollisions.
etherStatsDropEvents	Total number of drop events received 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 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 2/0/1
[Sysname-GigabitEthernet2/0/1] rmon statistics 1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1
- 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 takes 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 interval, 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 2/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] 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 2/0/1
[Sysname-GigabitEthernet2/0/1] rmon statistics 1
[Sysname-GigabitEthernet2/0/1] 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 GigabitEthernet2/0/1 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 GigabitEthernet 2/0/1
- 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. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, number of packets received. 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 2/0/1. The index of the entry is 20, and the owner of the entry is **user1**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] rmon statistics 20 owner user1
```

Table of Contents

1 MAC Address Table Management Configuration Commands

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: Displays blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match 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 00e0-fc01-0101.

```
<Sysname> display mac-address 00e0-fc01-0101
```

```
MAC ADDR       VLAN ID  STATE          PORT INDEX               AGING TIME(s)
00e0-fc01-0101 1        Config static Ethernet2/0/2           NOAGED
  ---  1 mac address(es) found  ---
```

Table 1-1 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: 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.

display mac-address mac-learning

Syntax

display mac-address mac-learning [*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. Displays MAC address learning status of the specified interface.

Description

Use the **display mac-address mac-learning** command to display MAC address learning status of the specified or all Ethernet ports.

Examples

Display MAC address learning status of port GigabitEthernet 2/0/1.

```
<Sysname> display mac-address mac-learning gigabitethernet 2/0/1
Mac address learning status of the switch: enable
PortName                        Learning Status
GigabitEthernet2/0/1               enable
```

Table 1-2 display mac-address mac-learning command output description

Field	Description
Mac address learning status of the switch	Global MAC address learning status, enabled or disabled
PortName	Port name
Learning Status	MAC address learning status for a port, enabled or disabled

mac-address (Ethernet 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 Ethernet port.

Use the **undo mac-address** command to remove a MAC address entry on the Ethernet port.

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.
- You cannot configure a static or dynamic MAC address entry on an aggregation port.

Related commands: **display mac-address**.

Examples

Add a static entry for MAC address 00e0-fc01-0101 on port GigabitEthernet 2/0/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] mac-address static 00e0-fc01-0101 vlan 2
```

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: Blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match 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.

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 00e0-fc01-0101. All frames destined to this MAC address are sent out of port GigabitEthernet 2/0/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 00e0-fc01-0101 interface gigabitethernet 2/0/1 vlan 2
```

mac-address mac-learning disable

Syntax

mac-address mac-learning disable

undo mac-address mac-learning disable

View

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

Default Level

2: System level

Parameters

None

Description

Use the **mac-address mac-learning disable** command to disable MAC address learning globally, on one or a group of Ethernet ports, or on a Layer-2 aggregate interface, depending on the view you entered.

Use the **undo mac-address mac-learning disable** command to enable MAC address learning globally, on one or a group of Ethernet ports, or on a VLAN, depending on the view you entered.

By default, MAC address learning is enabled globally and on all Ethernet ports.

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

When MAC address learning is disabled, the learned MAC addresses remain valid until they age out.

Examples

Disable global MAC address learning.

```
<Sysname> system-view
[Sysname] mac-address mac-learning disable
```

Disable MAC address learning on port GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] mac-address mac-learning disable
```

mac-address max-mac-count

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, in the range 0 to 4096. When the argument takes 0, the VLAN is not allowed to learn MAC addresses.

Description

Use the **mac-address max-mac-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 remove the restriction on the maximum number of MAC addresses that can be learned on an Ethernet port.

By default, no maximum number of MAC addresses that can be learned on a port is 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.

By using this command with the static MAC address function, you can disable an interface or a port group from learning MAC addresses, and only allow the packets with the specified destination address to pass, thus avoiding the access to the network from the illegal devices.

Note

The Layer-2 aggregate interface and member interface not support this function.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

Examples

Set the maximum number of MAC addresses that can be learned on port GigabitEthernet 2/0/1 to 600. After this upper limit is reached, frames received with unknown destination MAC addresses on the port will not be forwarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] mac-address max-mac-count 600
```

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,in the range 10 to 86400.

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
```

Table of Contents

1 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 to extend the value 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.

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

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.

Examples

Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
  PING 2001::1 : 56  data bytes, press CTRL_C to break
  Reply from 2001::1  bytes=56 Sequence=1 hop limit=64  time = 20 ms
  Reply from 2001::1  bytes=56 Sequence=2 hop limit=64  time = 0 ms
```

```
Reply from 2001::1  bytes=56 Sequence=3 hop limit=64  time = 0 ms
Reply from 2001::1  bytes=56 Sequence=4 hop limit=64  time = 0 ms
Reply from 2001::1  bytes=56 Sequence=5 hop limit=64  time = 0 ms
--- 2001::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/4/20 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.

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 routers 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 routers the packets traverse from the source to the destination device. If a router times out, "* * *" will be displayed.

Examples

Display the routers 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
```

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 routers the IPv6 packets traverse from the source to the destination device.

Examples

View the routes involved for packets to travel 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
 1 3003::1 30 ms 10 ms 10 ms
 2 3002::1 10 ms 11 ms 9 ms
```

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
```

Table of Contents

1 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 1-1 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
Log file	9	channel9

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
```

Table 1-2 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 1-4 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 1-4 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 1-4 for details.

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).

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
logfile:
    channel number:9, channel name:channel9
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date
```

Table 1-3 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

Field	Description
SNMP Agent: channel number : 5, channel name : snmpagent	Configurations on the SNMP module destination, including the channel number and channel name used
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.
logfile: channel number:9, channel name:channel9	Configurations on the log file destination, including 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** *slotnum*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

reverse: Displays log information from new to old. If this keyword is not specified, the log information will be displayed from old to new.

level *severity*: Displays information of the log with specified level, where *severity* represents information level, in the range 0 to 7.

Table 1-4 Severity description

Severity	Value	Description
emergencies	0	The system is unavailable
alerts	1	Information that requires prompt reaction

Severity	Value	Description
critical	2	Critical information
errors	3	Error information
warnings	4	Warnings
notifications	5	Normal errors with important information
informational	6	Informational information to be recorded
debugging	7	Debugging information

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 *slotnum*: Slot number.

|: 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.

```
<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 : 0
Current messages : 127

%Jun 19 18:03:24:55 2006 Sysname IC/7/SYS_RESTART:
System restarted --
```

The rest is omitted here.

Table 1-5 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.

Field	Description
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
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** *slotnum*] *

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 *slotnum*: Slot number.

Description

Use the **display logbuffer summary** command to display the summary of the log buffer.

Examples

Display the summary of the log buffer.

```
<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 1-6 display logbuffer summary command output description

Field	Description
SLOT	Slot number
EMERG	Represents emergencies, refer to Table 1-4 for details

Field	Description
ALERT	Represents alerts, refer to Table 1-4 for details
CRIT	Represents critical, refer to Table 1-4 for details
ERROR	Represents errors, refer to Table 1-4 for details
WARN	Represents warnings, refer to Table 1-4 for details
NOTIF	Represents notifications, refer to Table 1-4 for details
INFO	Represents informational, refer to Table 1-4 for details
DEBUG	Represents debugging, refer to Table 1-4 for details

display logfile buffer

Syntax

display logfile buffer

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display logfile buffer** command to display contents of the logfile buffer.

Note that all contents in the logfile buffer will be cleared after they are successfully saved into the log file automatically or manually.

Examples

Display the contents of the log file buffer.

```
<Sysname> display logfile buffer
%@387986%Jun 20 10:52:03 2006 Sysname %%10IC/7/SYS_RESTART:
System restarted --
```

The rest is omitted here.

display logfile summary

Syntax

display logfile summary

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display logfile summary** command to display the configuration of the log file.

Examples

Display the configuration of the log file.

```
<Sysname> display logfile summary
  Log file is enabled.
  Channel number : 9
  Log file size quota : 10 MB
  Log file directory : flash:/logfile
  Writing frequency : 24 hour 0 min 10 sec
```

Table 1-7 display logfile summary command output description

Field	Description
Log file is	The current state of a log file, which could be enabled or disabled.
Channel number	The channel number of a log file, defaults to 9.
Log file size quota	The maximum storage space reserved for a log file
Log file directory	Log file directory
Writing frequency	Log file writing frequency

display trapbuffer

Syntax

display trapbuffer [**reverse**] [**size** *buffersize*]

View

Any view

Default Level

1: Monitor level

Parameters

reverse: Displays trap messages from new to old. If this keyword is not specified, trap messages will be displayed from old to new.

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 : 1

#Dec 31 14:01:25 2004 Sysname DEV/2/LOAD FINISHED:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.20: frameIndex is 0, slotIndex 0.4
```

Table 1-8 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 Ethernet 2/0/1 from generating link up/down logging information.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 1-1 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 logfile enable

Syntax

info-center logfile enable

undo info-center logfile enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **info-center logfile enable** command to enable the output of system information to the log file.

Use the **undo info-center logfile enable** command to disable the output of system information to the log file.

By default, the output of system information to the log file is enabled.

Examples

Enable the logfile feature.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

View

System view

Default Level

2: System level

Parameters

freq-sec: Frequency with which the system saves the log file, in the range 1 to 86,400 seconds. The default value is 86,400.

Description

Use the **info-center logfile frequency** command to configure the frequency with which the system saves the log file.

Use the **undo info-center logfile frequency** command to restore the default frequency.

Examples

Configure the frequency with which the system saves the log file as 60,000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

info-center logfile size-quota

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

View

System view

Default Level

2: System level

Parameters

size: The maximum capacity of a disk, in MB. The value, however, cannot be smaller than 1 MB and larger than 10 MB. The default value is 1.

Description

Use the **info-center logfile size-quota** command to set the maximum storage space reserved for a log file.

Use the **undo info-center logfile size-quota** command to restore the default maximum storage space reserved for a log file.

Examples

Set the maximum storage space reserved for a log file to 6 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 6
```

info-center logfile switch-directory

Syntax

info-center logfile switch-directory *dir-name*

View

System view

Default Level

2: System level

Parameters

dir-name: The name of the directory where a log file is saved, a string of 1 to 64 characters.

Description

Use the **info-center logfile switch-directory** command to configure the directory where a log file is saved. Ensure that the directory is created first before saving a log file into it.

By default, the directory to save a log file is the logfile directory under the root directory of the storage device. For a device supporting CF partition, the directory to save a log file is the logfile directory in the second partition of the storage device.

Note that this command can be used to configure the directory to which a log file can be saved. The configuration will lose after system restart or active/standby switchover of the main control boards.

Examples

Create a directory with the name **test** under flash root directory.

```
<Sysname> mkdir test
%Created dir flash:/test.
```

Set the directory to save the log file to flash:/test.

```
<Sysname> system-view
[Sysname] info-center logfile switch-directory flash:/test
```

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

Set to 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

Configure interface VLAN-interface 1 as the egress interface to output log information to the log host.

```
<Sysname> system-view
[Sysname] info-center loghost source Vlan-interface 1
```

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

Set to 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

Set to 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 1-4 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 1-9.

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 warnings 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 the modules without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the modules are used. Refer to Table 1-9 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 debugging. 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 1-9 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	warnings	Enabled	debugging	Enabled	debugging
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP module	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging
Log file	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging

Examples

Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergencies**. 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 **emergencies**. 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 ethe** command to view Ethernet interface information.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
```

```
[Sysname] display interface ethe
```

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 ethe** in this example.

```
%Apr 29 08:12:44:71 2007 Sysname IFNET/4/LINK UPDOWN:
 Ethernet2/0/1: link status is UP
[Sysname] display interface ethe
```

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]:
```

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.

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 Ethernet 2/0/1 that is in the UP state, the log information generated is as follows:

```
%0.1382605158 Sysname IFNET/4/LINK UPDOWN:
 Ethernet2/0/1: 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 Ethernet 2/0/1 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:
 Ethernet2/0/1: 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 Ethernet 2/0/1 that is in the UP state, the log information generated is as follows:

```
% Sysname IFNET/4/LINK UPDOWN:
 Ethernet2/0/1: 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, the format of which 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
```

logfile save

Syntax

logfile save

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **logfile save** command to save all the contents in the logfile buffer into the log file.

By default, the system automatically saves the log file based on a frequency configured by the **info-center logfile frequency** command into a directory configured by the **info-center logfile switch-directory** command.

Note that all contents in the logfile buffer will be cleared after they are successfully saved into the log file automatically or manually.

 **Note**

By default, the log file is automatically saved to the logfile directory under root directory of the CF card (cf:/logfile). If there is no CF card, you can use the **info-center logfile switch-directory** command to configure the directory where a log file is saved, otherwise, the system will prompt you that the save operation failed.

Examples

Save the contents in the logfile buffer into the log file.

```
<Sysname> logfile save
```

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
```

Table of Contents

1 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] apply poe-profile name A20
[Sysname-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 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 Ethernet 2/0/1.

```
<Sysname> system-view
[Sysname] apply poe-profile name ABC interface ethernet 2/0/1
```

Apply the indexed PoE configuration file to PoE interfaces Ethernet 2/0/2 through Ethernet 2/0/8.

```
<Sysname> system-view
[Sysname] apply poe-profile name ABC interface ethernet 2/0/2 to ethernet 2/0/8
```

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 slot of all the power sourcing equipments (PSEs).

Examples

Display the mapping between ID, module, and slot of each PSE. (The information displayed depends on the device model.)

```
<Sysname> display poe device
 PSE ID  SlotNo SubSNo PortNum  MaxPower(W)  State  Model
 19      6      0      48       37           off    LSQ1FV48SA
```

Table 1-1 display poe device command output description

Field	Description
PSE ID	ID of the PSE
SlotNo	Slot number of the PSE
SubSNo	Sub Slot number
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 Ethernet 2/0/1.

```
<Sysname> display poe interface ethernet 2/0/1
 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                     : 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 1-2 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 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 Power Mode	Power mode of a PoE interface: • signal: Power is supplied over signal cables. • spare: Power is supplied over spare cables.
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.
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
 GE2/0/1   enable   low       4.4       on           1      delivering-power
 GE2/0/2   enable   critical  0         on           -      disabled
 GE2/0/3   enable   low       0         on           -      disabled
 GE2/0/4   enable   critical  0         on           -      searching
 GE2/0/5   enable   low       4.0       on           2      delivering-power
 GE2/0/6   enable   low       0         on           -      disabled
 GE2/0/7   disable  low       0         off          -      fault
 GE2/0/8   disable  low       0         off          -      disabled
 GE2/0/9   disable  low       0         off          -      disabled
 GE2/0/10  disable  low       0         off          -      disabled
 GE2/0/11  disable  low       0         off          -      disabled
 GE2/0/12  disable  low       0         off          -      disabled

 ---  2 port(s) on,    8.4(W) consumed,   791.6(W) Remaining ---
```

Table 1-3 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 Ethernet 2/0/1.

```
<Sysname> display poe interface power ethernet 2/0/1
Interface  CurPower PeakPower MaxPower PD Description
           (W)      (W)       (W)
 Eth2/0/1   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)
 GE2/0/25   4.4       4.5      4.6       IP Phone on Room 309 for Peter Smith
 GE2/0/26   4.4       4.5      15.4      IP Phone on Room 409 for Peter Pan
 GE2/0/27   15.0     15.3      15.4     Acess Point on Room 509 for Peter
 GE2/0/28   0         0         0        IP Phone on Room 609 for Peter John
 GE2/0/29   0         0         0        IP Phone on Room 709 for Jack
 GE2/0/30   0         0         0        IP Phone on Room 809 for Alien

---  3 port(s) on,   23.8(W) consumed,   776.2(W) Remaining ---
```

Table 1-4 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 power-usage

Syntax

display poe power-usage

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe power-usage** command to display the power information of the PoE power and all PSEs

Examples

Display the power information of the PoE power and all PSEs.

```
<Sysname> display poe power-usage
PoE Current Power               : 600   W
PoE Max Power                   : 2000  W
PoE Max Guaranteed Power        : 1000  W
PoE Remaining Allocate Power    : 800   W
PoE Remaining Guaranteed Power  : 600   W
PoE Total Powered Port Number   : 60
Detailed power usage of PSE(s):
PSE ID   Max    Current    Peak    Average    Remaining         Powered
        (W)     (W)        (W)     (W)        Guaranteed(W)     PortNum
10       300     200        230     205        100               20
13       500     100        120     110        300               10
```

Table 1-5 display poe power-usage command output description

Field	Description
PoE Current Power	Total consumption power of the PSE
PoE Max Power	Maximum PoE power
PoE Max Guaranteed Power	Guaranteed maximum PoE power, namely, the maximum power supplied to critical PSEs
PoE Remaining Allocate Power	Remaining allocable PoE power = Maximum PoE power – the sum of the maximum power of all PoE-enabled PSEs
PoE Remaining Guaranteed Power	Guaranteed remaining PoE power = Guaranteed maximum PoE power – the sum of the maximum power of critical PSEs
PoE Total Powered Port Number	Number of PoE interfaces that are currently supplying power

Field	Description
PSE ID	ID of the PSE
Max	Maximum power of the PSE
Current	Current power of the PSE
Peak	Peak power of the PSE
Average	Average power of the PSE
Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE – the sum of the maximum power of critical PoE interfaces of the PSE
Powered PortNum	Number of PoE interfaces for which the PSE is supplying power

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 slot. 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 7.

```
<Sysname> display poe pse 7
 PSE ID                        : 7
 PSE Slot No                   : 2
 PSE Model                      : LSQ1FV48SA
 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 Pse-policy Mode              : disable
PSE Pd-policy Mode              : disable
PSE PD Disconnect Detect Mode    : AC
```

Table 1-6 display poe pse command output description

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Slot number of the PSE
PSE Model	Model of the PSE module
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 Pse-policy Mode	PSE power management policy mode
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 slot.

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 7.

```
<Sysname> display poe pse 7 interface
<Sysname> display poe pse 7 interface
 Interface  Enable   Priority  CurPower  Operating   IEEE   Detection
                               (W)       Status      class  Status
 GE2/0/1      enable   low       4.4       on          1     delivering-power
 GE2/0/2      enable   critical  0         power-lack  -     disabled
 GE2/0/3      enable   low       0         power-deny  -     disabled
 GE2/0/4      enable   critical  0         on          -     searching
 GE2/0/5      enable   low       4.0       power-limit 2     delivering-power
 GE2/0/6      enable   low       0         power-itself -    disabled
 GE2/0/7      disable  low       0         off          -    fault
 GE2/0/8      disable  low       0         off          -    disabled
 GE2/0/9      disable  low       0         off          -    disabled
 GE2/0/10     disable  low       0         off          -    disabled
 GE2/0/11     disable  low       0         off          -    disabled
 GE2/0/12     disable  low       0         off          -    disabled

 ---  2 port(s) on,    8.4(W) consumed,   171.6(W) Remaining ---
```

Table 1-7 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 1-2.
Priority	Priority of a PoE interface. For the value, see Table 1-2.
CurPower	Current power of a PoE interface
Operating	Operating state of a PoE interface. For the value, see Table 1-2.
IEEE	PD power class
Detection	Power detection state of a PoE interface. For the value, see Table 1-2.

Field	Description
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 slot.

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 7.

```
<Sysname> display poe pse 7 interface power
Interface  CurPower PeakPower MaxPower PD Description
           (W)      (W)       (W)
 GE2/0/25   4.4       4.5       4.6      IP Phone on Room 309 for Peter Smith
 GE2/0/26   4.4       4.5       15.4     IP Phone on Room 409 for Peter Pan
 GE2/0/27   15.0      15.3      15.4     Acess Point on Room 509 for Peter
 GE2/0/28   0         0         5        IP Phone on Room 609 for Peter John
 GE2/0/29   0         0         4        IP Phone on Room 709 for Jack
 GE2/0/30   0         0         5        IP Phone on Room 809 for Alien

---  3 port(s) on,   23.8(W) consumed,   776.2(W) Remaining ---
```

Table 1-8 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

Field	Description
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-power

Syntax

display poe-power

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power** command to display the information of the PoE power.

Examples

Display information of the PoE power.

```
<Sysname> display poe-power
 PoE Current Power          : 1870    W
 PoE Average Power          : 2100    W
 PoE Peak Power             : 2350    W
 PoE Max Power              : 2000    W
 PoE Nominal Power          : 2500    W
 PoE Current Current        : 3.00    A
 PoE Current Voltage        : 55.00   V
 PoE Input-threshold Lower  : 111.22  V
 PoE Input-threshold Upper  : 131.00  V
 PoE Output-threshold Lower : 45.00   V
 PoE Output-threshold Upper : 57.00   V
 PoE Hardware Version       : 0002
 PoE Software Version       : 0001
 PoE Power Number           : 2
 PoE Power 1:
    Manufacturer          : Tyco Electronics Com
    Type                  : PSE2500-A
```

```
    Status                : Normal
PoE Power 2:
    Manufacturer          : Tyco Electronics Com
    Type                  : PSE2500-B
    Status                : Normal
```

Table 1-9 display poe-power command output description

Field	Description
PoE Current Power	Current PoE power
PoE Average Power	Average PoE power
PoE Peak Power	Peak PoE power
PoE Max Power	Maximum PoE power
PoE Nominal Power	Nominal PoE power
PoE Current Current	Current PoE current
PoE Current Voltage	Current PoE voltage
PoE Input-threshold Lower	AC input under-voltage threshold
PoE Input-threshold Upper	AC input over-voltage threshold
PoE Output-threshold Lower	DC output under-voltage threshold
PoE Output-threshold Upper	DC output over-voltage threshold
PoE Hardware Version	PoE hardware version number
PoE Software Version	PoE software version number
PoE Power Number	Number of PoE power supply units
Manufacturer	Manufacturer of the PoE power. If the device does not support to get this field, it is displayed as NONE.
Type	Type of the PoE power. If the device does not support to get this field, it is displayed as NONE.
PoE Power Status	PoE power state: • Normal • Absent • Off • Master • Slave • Balance • Redundant • Alarm • Faulty The PoE power state varies with devices.

display poe-power ac-input state

Syntax

display poe-power ac-input state

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power ac-input state** command to display the state information of the AC input power.

Examples

Display the state information of the AC input power.

```
<Sysname> display poe-power ac-input state
Module Number              : 2
Output AC Current A Alarm  : Normal
Output AC Current B Alarm  : Under Limit
Output AC Current C Alarm  : Lack Phase
Module 1:
   Volt Phase AB Alarm     : Above Limit
   Volt Phase BC Alarm     : Fuse Broken
   Volt Phase CA Alarm     : Switch Off
Module 2:
   Volt Phase AB Alarm     : Above Limit
   Volt Phase BC Alarm     : Fuse Broken
   Volt Phase CA Alarm     : Switch Off
```

Table 1-10 display poe-power ac-input state command output description

Field	Description
Module Number	Number of modules that a power supply unit (PSU) contains
Output AC Current A/B/C Alarm	Output three-phase AC voltage state: • Normal: The voltage is normal. • Under Limit: The voltage is below the lower limit. • Above Limit: The voltage is above the upper limit. • Lack Phase: A phase is lost. • Fuse Broken: The fuse is broken. • Switch Off: The switch is turned off. • Other Error: Other faults
Volt Phase AB/BC/CA Alarm	AC voltage input state: Same as those of the output three-phase AC current

display poe-power alarm

Syntax

display poe-power alarm

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power alarm** command to display the alarm information of the PoE power.

Examples

Display the alarm information of the PoE power.

```
<Sysname> display poe-power alarm
 PSU Number                : 3
 PSU 1 State               : Normal
 PSU 2 State               : Disconnect
 PSU 3 State               : Over Voltage
                             Over Temperature
```

Table 1-11 display poe-power alarm command output description

Field	Description
PSU Number	Number of PSUs
PSU x State	PSU state: • Normal: The PSU is normal. • Disconnect: The PSU is disconnected. • Input Error: An input error occurs to the PSU. • Output Error: An output error occurs to the PSU. • Over Voltage: An over-voltage occurs to the PSU. • Over Temperature: An over-temperature occurs to the PSU. • Fan Error: A fault occurs to the fan of the PSU. • Shut Down: The PSU is shut down. • Current Restricted: The current of the PSU is restricted.

display poe-power dc-output state

Syntax

display poe-power dc-output state

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power dc-output state** command to display the state information of the DC output power

Examples

Display the state information of the DC output power.

```
<Sysname> display poe-power dc-output state
DC Output State            : Normal
```

Table 1-12 display poe-power dc-output state command output description

Field	Description
DC Output State	DC output state. See Table 1-10.

display poe-power dc-output value

Syntax

display poe-power dc-output value

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power dc-output value** command to display the parameter values of the DC output power.

Examples

Display the parameter values of the DC output power.

```
<Sysname> display poe-power dc-output value
 DC Output Voltage         : 54.05 V
 DC Output Current         : 0.35  A
```

Table 1-13 display poe-power dc-output value command output description

Field	Description
DC Output Voltage	DC output voltage
DC Output Current	DC output current

display poe-power status

Syntax

display poe-power status

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power status** command to display the status information of the PoE power.

Examples

Display the status information of the PoE power.

```
<Sysname>display poe-power status
Switch Number             : 1
Switch 1 State            : AC Switch High Voltage
DC Output State           : Under Limit
DC Output Voltage         : 56.00   V
DC Output Current         : 15.00   A
Module Number             : 2
Output AC Current A Alarm  : Normal
Output AC Current B Alarm  : Under Limit
Output AC Current C Alarm  : Lack Phase
Module 1:
   Volt Phase AB Alarm   : Above Limit
   Volt Phase BC Alarm   : Fuse Broken
   Volt Phase CA Alarm   : Switch Off
Module 2:
   Volt Phase AB Alarm   : Above Limit
   Volt Phase BC Alarm   : Fuse Broken
   Volt Phase CA Alarm   : Switch Off
```

Table 1-14 display poe-power status command output description

Field	Description
Switch Number	Number of power switches
Switch x State	State of a power switch
DC Output State	DC output state
DC Output Voltage	DC output voltage
DC Output Current	DC output current
Module Number	Number of modules that a PSU contains
Output AC Current A/B/C Alarm	Output three-phase AC current state. See Table 1-10.
Volt Phrase AB/BC/CA Alarm	AC voltage input state. See Table 1-10.

display poe-power supervision-module

Syntax

display poe-power supervision-module

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power supervision-module** command to display the information of the monitoring module of the PoE power.

Examples

Display the information of the monitoring module of the PoE power.

```
<Sysname> display poe-power supervision-module
 Supervision Version        : 2.6
 Supervision Name           : Summer Pms
 PoE Power Type             : PSE2500-A
 PoE Current Power          : 600   W
 PoE Average Power          : 630   W
PoE Peak Power              : 650   W
 PoE Nominal Power          : 2400  W
 PSU Available Number       : 1
PSU 1:
    Nominal Output Power    : 2500(W)(220V)/1250(W)(110V)
    Hardware Version Info   : NP Series
```

Table 1-15 display poe-power supervision-module command output description

Field	Description
Supervision Version	Software version number of the monitoring module of the PoE power
Supervision Name	Name of the monitoring module of the PoE power
PoE Power Type	Type of the PoE power
PoE Current Power	Current consumption power
PoE Average Power	Average power
PoE Peak Power	Peak power
PoE Nominal Power	Nominal power
PSU Available Number	Number of available PSUs
Nominal Output Power	Nominal output power of a PSU
Hardware Version Info	Hardware version information of the PSU

display poe-power switch state

Syntax

display poe-power switch state

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe-power switch state** command to display the switch information of the PoE power.

Examples

Display the switch information of the PoE power.

```
<Sysname> display poe-power switch state
Switch Number             : 1
Switch 1 State            : AC Switch High Voltage
```

Table 1-16 display poe-power switch state command output description

Field	Description
Switch Number	Number of power switches
Switch x State	Switch state: • AC Switch On: The AC switch is turned on. • AC Switch Off: The switch is turned off. • AC Switch High Voltage: The voltage of the AC switch is high. • AC Switch Low Voltage: The voltage of the AC switch is low.

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         GE2/0/1     poe enable
                                  GE2/0/2     poe priority critical
                                  GE2/0/3

 poe-profileAA    2     1         GE2/0/24    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 1-17 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          GE2/0/2    poe enable
                                   GE2/0/24   poe priority critical
                                              poe max-power 12300

 ---  2 port(s) applied  ---
```

Table 1-18 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         GE2/0/1    poe enable
                                  GE2/0/2    poe priority critical
                                             poe max-power 12300

---  2 port(s) applied  ---
```

Table 1-19 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 Ethernet 2/0/1.

```
<Sysname> display poe-profile interface ethernet 2/0/1
Poe-profile     Index  ApplyNum  Interface  Current Configuration
AA3456789012345 1      2         Eth2/0/2   poe enable
                                            poe priority critical
```

Table 1-20 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

Field	Description
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 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 ethernet 2/0/1
```

```
[Sysname-Ethernet2/0/1] 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] apply poe-profile name abc
```

poe enable pse

Syntax

poe enable pse *pse-id*

undo poe enable pse *pse-id*

View

System view

Default Level

2: System level

Parameters

pse-id: PSE ID.

Description

Use the **poe enable pse** command to enable PoE for the PSE.

Use the **undo poe enable pse** command to disable PoE for the PSE.

By default, PoE is disabled for the PSE.

Examples

Enable PoE for PSE 7.

```
<Sysname> system-view
[Sysname] poe enable pse 7
```

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 7to detect nonstandard PDs.

```
<Sysname> system-view
[Sysname] poe legacy enable pse 7
```

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 Ethernet 2/0/1 to 12,000 milliwatts.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] poe max-power 12000
```

Set the maximum power of Ethernet 2/0/1 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 ethernet 2/0/1
```

```
[Sysname-Ethernet2/0/1] apply poe-profile name abc
```

poe max-power (system view)

Syntax

poe max-power *max-power* [**pse** *pse-id*]

undo poe max-power [**pse** *pse-id*]

View

System view

Default Level

2: System level

Parameters

max-power: Maximum power in watts of the PSE. Support for the range and default value of this argument depends on the device model.

pse *pse-id*: Specifies a PSE ID.

Description

Use the **poe max-power** command to configure the maximum power for the PSE.

Use the **undo poe max-power** command to restore the default maximum power of the PSE.

The default maximum power of the PSE is 806 watts.

Note that:

- The maximum power of the PSE must be greater than or equal to the sum of the maximum power of all critical PoE interfaces on the PSE so as to guarantee the power supply to these PoE interfaces. When the consumption power of all PDs connected to the PSE is greater than the maximum power of the PSE, some PDs will be powered off.
- The sum of the maximum power of all PSEs cannot exceed the maximum PoE power.

Related commands: **poe priority (system view)**.

Examples

Set the maximum power of PSE 7 to 150 watts.

```
<Sysname> system-view
[Sysname] poe max-power 150 pse 7
```

poe mode

Syntax

poe mode { **signal** | **spare** }

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).

spare: Specifies the PoE mode as **spare** (power over spare 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.

Examples

Set the PoE mode to **signal** (power over signal cables).

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 Ethernet 2/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] 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 power max-value

Syntax

poe power max-value *max-power*

undo poe power max-value

View

System view

Default Level

2: System level

Parameters

max-power: Maximum PoE power, namely, maximum power that the device can provide for all PSEs. In consideration of the transient peak power effect, the maximum power available is 5% higher than the configured maximum power. The range, default value, granularity, and limit vary with devices.

Description

Use the **poe power max-value** command to configure the maximum PoE power.

Use the **undo poe power max-value** command to restore the default.

The default maximum PoE power varies with devices.

Note that the configured maximum PoE power cannot exceed the rated PoE power.

Examples

Set the maximum PoE power to 2,000 watts for the device.

```
<Sysname> system-view
[Sysname] poe power max-value 2000
```

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 Ethernet 2/0/1 to **critical**.

```
<Sysname> system-view
[Sysname] interface ethernet 2/0/1
[Sysname-Ethernet2/0/1] poe priority critical
```

Set the power priority of Ethernet 2/0/1 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 ethernet 2/0/1
[Sysname-Ethernet2/0/1] apply poe-profile name abc
```

poe priority (system view)

Syntax

poe priority { **critical** | **high | low** } [**pse** *pse-id*]

undo poe priority [**pse** *pse-id*]

View

System view

Default Level

2: System level

Parameters

critical: Sets the power priority level of the PSE to **critical**. The PSE whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PSE.

high: Sets the power priority of the PSE to **high**.

low: Sets the power priority of the PSE to **low**.

pse *pse-id*: Specifies a PSE ID.

Description

Use the **poe priority** command to configure a power priority level for the PSE.

Use the **undo poe priority** command to restore the default.

By default, the power priority level of the PSE is **low**.

When the PoE power is insufficient, power is first supplied to PSE with a higher power priority level.

Examples

Set the power priority of PSE 7 to **critical**.

```
<Sysname> system-view
[Sysname] poe priority critical pse 7
```

poe pse-policy priority

Syntax

poe pse-policy priority

undo poe pse-policy priority

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **poe pse-policy priority** command to configure a PSE power management priority policy.

Use the **undo poe pse-policy priority** command to remove the PSE power management priority policy.

By default, no PSE power management priority policy is configured.

Examples

Configure a PSE power management priority policy.

```
<Sysname> system-view
[Sysname] poe pse-policy priority
```

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).
- If you upgrade the PSE firmware on a backup control board, the upgrade file must be on the main control board, and only the main control board can control the upgrade of the PSE firmware on the backup control board.

Examples

Upgrade the processing software of PSE 7 online.

```
<Sysname> system-view
[Sysname] poe update refresh 0400_001.S19 pse 7
```

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 7 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 7
```

poe-power input-threshold

Syntax

poe-power input-threshold { **lower** | **upper** } *value*

undo poe-power input-threshold { **lower** | **upper** }

View

System view

Default Level

2: System level

Parameters

lower *value*: Specifies an under-voltage threshold in volts. The under-voltage threshold range, default under-voltage threshold, and recommended under-voltage threshold vary with devices.

upper *value*: Specifies an over-voltage threshold in volts. The over-voltage threshold range, default over-voltage threshold, and recommended over-voltage threshold vary with devices.

Description

Use the **poe-power input-threshold** command to configure an AC input under-voltage/over-voltage threshold.

Use the **undo poe-power input-threshold** command to restore the default.

The default AC input under-voltage/over-voltage threshold varies with devices.

Examples

Set the AC input under-voltage threshold to 181 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold lower 181
```

Set the AC input over-voltage threshold to 264 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold upper 264
```

poe-power output-threshold

Syntax

poe-power output-threshold { **lower** | **upper** } *value*

undo poe-power output-threshold { **lower** | **upper** }

View

System view

Default Level

2: System level

Parameters

lower *value*: Specifies an under-voltage threshold in volts. The under-voltage threshold range, default under-voltage threshold, and recommended under-voltage threshold vary with devices.

upper *value*: Specifies an over-voltage threshold in volts. The over-voltage threshold range, default over-voltage threshold, and recommended over-voltage threshold vary with devices.

Description

Use the **poe-power output-threshold** command to configure a DC output under-voltage/over-voltage threshold.

Use the **undo poe-power output-threshold** command to restore the default.

The default DC output under-voltage/over-voltage threshold varies with devices.

Examples

Set a DC output under-voltage threshold to 45 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold lower 45
```

Set a DC output over-voltage threshold to 57 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold upper 57
```

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
```

Table of Contents

1 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 1-1 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
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 nqa** 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 for association with the specified Reaction entry of the NQA test group.

Note that after a Track object is created, you cannot modify it using the **track nqa** command. You have to remove it and create a new one.

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 NQA Configuration Commands

NQA Client Configuration Commands

data-fill

Syntax

data-fill *string*

undo data-fill

View

ICMP-echo, UDP-echo, UDP-jitter 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 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 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 a probe packet is 3 byte, **abc** is used to fill the packet. When the probe size 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 a probe packet have some specific usage, the configured character string is used to fill the remaining bytes in the probe packet.
- In a UDP-jitter test, because the first 68 bytes of a probe packet have some specific usage, the configured character string is used to fill the remaining bytes in the probe 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 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 and in the range 68 to 8100 for a UDP-jitter test.

Description

Use the **data-size** command to configure the size of a probe packet sent.

Use the **undo data-size** command to restore the default.

By default, the size of a probe packet is 100 bytes.

- For an ICMP-echo test, the size of a packet sent in a probe is the length of the data field in an ICMP echo message.
- For a UDP-echo test and UDP-jitter test, the size of a packet sent in a probe 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 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 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 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

Syntax

display nqa { **result** | **history** } [*admin-name operation-tag*]

View

Any view

Default Level

2: System level

Parameters

result: Displays the results of the last test.

history: Displays the history records of a test.

admin-name: Specifies the name of the administrator who creates NQA operations, 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.

Description

Use the **display nqa** command to display operation information of an NQA test or tests.

If neither of the test group arguments (*admin-name* and *operation-tag*) is specified, information of all test groups is displayed.

Examples

Display the results of the last NQA test, in which the administrator name is **administrator**, and the operation tag is **jitter**.

```
<Sysname> display nqa result administrator jitter
  NQA entry(admin administrator, tag jitter) test results:
    Destination IP address: 192.168.0.81
      Send operation times: 10             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
    Extend results:
      Packet lost in test: 100%
      Failures due to timeout: 10
      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
    UDP-jitter results:
     RTT number: 0
      SD max delay: 0                      DS max delay: 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
      SD lost packet(s): 0                 DS lost packet(s): 0
      Lost packet(s) for unknown reason: 10
```

Table 1-1 display nqa result command output description

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent

Field	Description
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time
Square-Sum of round trip time	Square sum of roundtrip time
Last succeeded probe time	Time of the last successful probe in a test
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
UDP-jitter results	UDP-jitter test results, available only in UDP-jitter tests.
RTT number	Number of response packets received
SD max delay	Maximum delay from the source to the destination
DS max delay	Maximum delay from the destination to the source
Min positive SD	Minimum positive jitter delay from the source to the destination
Min positive DS	Minimum positive jitter delay from the destination to the source
Max positive SD	Maximum positive jitter delay from the source to the destination
Max positive DS	Maximum positive jitter delay from the destination to the source
Positive SD number	Number of positive jitter delays from the source to the destination
Positive DS number	Number of positive jitter delays from the destination to the source
Positive SD sum	Sum of positive jitter delays from the source to the destination
Positive DS sum	Sum of positive jitter delays from the destination to the source
Positive SD average	Average of positive jitter delays from the source to the destination
Positive DS average	Average of positive jitter delays from the destination to the source
Positive SD square sum	Sum of the square of positive jitter delays from the source to the destination
Positive DS square sum	Sum of the square of positive jitter delays from the destination to the source
Min negative SD	Minimum absolute value of negative jitter delays from the source to the destination
Min negative DS	Minimum absolute value of negative jitter delays from the destination to the source
Max negative SD	Maximum absolute value of negative jitter delays from the source to the destination

Field	Description
Max negative DS	Maximum absolute value of negative jitter delays from the destination to the source
Negative SD number	Number of negative jitter delays from the source to the destination
Negative DS number	Number of negative jitter delays from the destination to the source
Negative SD sum	Sum of absolute values of negative jitter delays from the source to the destination
Negative DS sum	Sum of absolute values of negative jitter delays from the destination to the source
Negative SD average	Average absolute value of negative jitter delays from the source to the destination
Negative DS average	Average absolute value of negative jitter delays from the destination to the source
Negative SD square sum	Sum of the square of negative jitter delays from the source to the destination
Negative DS square sum	Sum of the square of negative jitter delays from the destination to the 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

Display the history records of tests, 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 1-2 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)

Field	Description
Status	Status value of test results, including: • Succeeded • Unknown error • Internal error • Timeout
Time	Time when the test is completed

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.

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 tests for a test group 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*.

Note

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 5.

```
<Sysname> system-view
[Sysname] nqa agent max-concurrent 5
```

nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time now 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.

now: Specifies to start the test for a test group immediately.

forever: Specifies that the test is performed for a test group forever.

Description

Use the **nqa schedule** command to configure the test start time and test period 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.
- At present, the configuration of the end time of an NQA test is not supported on the device, and you need to use the **undo nqa schedule** command to end an NQA test.

Examples

Start a test for the test group with the administrator name **admin** and operation tag **test**.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time now lifetime forever
```

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

Any NQA 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, 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.

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 test type view

Default Level

2: System level

Parameters

packet-interval: Interval for packets sent in a probe in a UDP-jitter test, in milliseconds, in the range 10 to 1000.

Description

Use the **probe packet-interval** command to configure the interval for sending packets in a probe in a UDP-jitter 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 test type view

Default Level

2: System level

Parameters

packet-number: Number of packets sent in a UDP-jitter test, in the range 10 to 1000.

Description

Use the **probe packet-number** command to configure the number of packets sent in a UDP-jitter probe.

Use the **undo probe packet-number** command to restore the default.

By default, the number of packets sent in a probe is 10.

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 test type view

Default Level

2: System level

Parameters

packet-timeout: Timeout time for waiting for responses in a UDP-jitter 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 test.

Use the **undo probe packet-timeout** command to restore the default.

By default, the timeout time in a UDP-jitter test is 3000 milliseconds.

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.

Related commands: **track** in the *Track Commands* in the *System 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.

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 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 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 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
```

tos

Syntax

tos *value*

undo tos

View

DLSw, FTP, HTTP, ICMP-echo, SNMP, TCP, UDP-echo, UDP-jitter 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 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** }

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.

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**.

```
<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 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, and UDP-echo 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 1-3 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**.

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**.

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 and UDP-echo 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**.

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
```

Table of Contents

1 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.

Description

Use the **display ntp-service sessions** command to view the information of all NTP sessions. Without the **verbose** keyword, this command will display only the brief information of all NTP service sessions.

Examples

View the brief information of NTP service 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 1-1 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

Field	Description
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: 2^17
 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 1-2 display ntp-service status command output description

Field	Description
Clock status	Status of the system clock
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
Actual frequency	The actual frequency of the local system hardware clock
Clock precision	The precision of the system clock
Clock offset	The offset of the system clock relative to the reference source
Root delay	The roundtrip delay from the local device to the primary reference source
Root dispersion	The maximum error of the system clock relative to the primary reference source
Peer dispersion	The maximum error of the system clock relative to the reference source
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 1-3 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
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.

query: Specifies to permit control query.

server: Specifies to permit server access and query.

synchronization: Specifies to permit server access only.

acl-number: Basic ACL number, in the range of 2000 to 2999

Description

Use the **ntp-service access** command to configure the NTP service access-control right to 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 local NTP service access-control right 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 perform an access-control right match and will use the first matched right.

Note

- The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication.
- Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.

Examples

Configure devices on the 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.

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.

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.

Examples

Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[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.

Use the **undo ntp-service broadcast-client** command to remove the configuration.

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.

Use the **undo ntp-service broadcast-server** command to remove the configuration.

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.

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. The value range is 224.0.1.0 to 224.0.1.255.

Description

Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode.

Use the **undo ntp-service multicast-client** command to remove the configuration.

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. The value range is 224.0.1.0 to 224.0.1.255.

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.

Use the **undo ntp-service multicast-server** command to remove the configuration.

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 refclock-master

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the local clock, which is 127.127.1.u, where u is the NTP process ID, in the range of 0 to 3. If you do not specify *ip-address*, it defaults to 127.127.1.0.

stratum: Stratum level of the local clock, in the range of 1 to 15 and defaulting to 8.

Description

Use the **ntp-service refclock-master** command to configure the local clock as a reference source for other devices.

Use the **undo ntp-service refclock-master** command to remove the configuration.

Note

The stratum level of a clock defines 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.

Examples

Specify the local clock as the reference source, with the stratum level of 3.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 3
```

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**, and specify that this key is a trusted key.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[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 an interface for sending NTP messages.

Use the **undo ntp-service source-interface** command to remove the configured interface for sending 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 a particular interface for sending all NTP messages, so that the source address in all NTP messages is the primary IP address of this interface.

Examples

Specify that all NTP messages are to be sent out from 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 host 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 an interface for sending 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 PE to a PE or CE 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, and configure the device to run NTP version 3, and send NTP messages through 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 host 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 an interface for sending 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 PE to a PE or CE 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
```

Table of Contents

1 VRRP Configuration Commands

Note

- The term switch in this document refers to a switch in a generic sense or a Layer 3 switch.
- At present, the interfaces that VRRP involves can only be VLAN interfaces unless otherwise specified.

IPv4-Based VRRP Configuration Commands

display vrrp

Syntax

display vrrp [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **display vrrp** command to display the state information of VRRP.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both an interface and a VRRP group, only the state information of the specified VRRP group is displayed; if you only specify an interface, the state information of all the VRRP groups on the interface is displayed; if you specify neither, the state information of all the VRRP groups on the device is displayed.

Examples

Display brief information about all VRRP groups on the device.

```
<Sysname> display vrrp
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Total number of virtual routers: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type        IP
 ------------------------------------------------------------------------
 Vlan100             1    Master      100     1       NONE     10.10.10.2
```

Display detailed information about all VRRP groups on the device.

```
<Sysname> display vrrp verbose
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Total number of virtual routers: 1
 Interface       : Vlan-interface100
 VRID            : 1                   Adver. Timer    : 1
 Admin Status    : UP                  State           : Master
 Config Pri      : 100                 Run Pri         : 100
 Preempt Mode    : YES                 Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Vlan200             Pri Reduced     : 10
 Track Object    : 1                   Pri Reduced     : 10
 Track Object    : 2                   Switchover
 Virtual IP      : 10.10.10.2
 Virtual MAC     : 0000-5e00-0101
 Master IP       : 10.10.10.1
```

Table 1-1 display vrrp command output description

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IP address of the VRRP group
Total number of virtual routers	Number of VRRP groups
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
Adver. Timer	VRRP advertisement interval
Admin Status	Administrative state: UP or DOWN
State	Status of the switch in the VRRP group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemptive mode
Delay Time	Preemption delay
Auth Type	Authentication type

Field	Description
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp vrid track interface** command.
Track Object	The object to be tracked. It is displayed only after the execution of the **vrrp vrid track** command.
Pri Reduced	The priority value that is reduced when the monitored interface is down or when the status of the monitored Track object turns to **negative**. It is displayed only after the execution of the **vrrp vrid track interface** command or the **vrrp vrid track** command.
Switchover	Switchover mode. If the status of the monitored Track object turns to **negative**, the backup will switch to the master immediately.
Virtual IP	Virtual IP addresses of the VRRP group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the VRRP group. It is displayed only when the switch is in the state of master.
Master IP	Primary IP address of the interface which belongs to the switch in the state of master

display vrrp statistics

Syntax

display vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays VRRP statistics of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **display vrrp statistics** command to display statistics about VRRP.

If you specify both an interface and a VRRP group, only the statistics about the specified VRRP group are displayed; if you only specify an interface, the statistics about all the VRRP groups on the interface are displayed; if you specify neither, the statistics about all the VRRP groups on the device are displayed.

Examples

Display the statistics about all VRRP groups.

```
<Sysname> display vrrp statistics
 Interface              : Vlan-interface100
 VRID                   : 1
 CheckSum Errors        : 16         Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 IP TTL Errors          : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 1          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 16         Priority Zero Pkts Sent       : 0
 Advertise Sent         : 40

 Interface              : Vlan-interface200
 VRID                   : 105
 CheckSum Errors        : 0          Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 IP TTL Errors          : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 0          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent       : 0
 Advertise Sent         : 30

Global statistics
 CheckSum Errors        : 16
 Version Errors         : 0
 VRID Errors            : 20
```

Table 1-2 display vrrp statistics command output description

Field	Description
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IP address list errors
Become Master	Number of times that the switch worked as the master

Field	Description
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all VRRP groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp statistics

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

User view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears VRRP statistics of a specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **reset vrrp statistics** command to clear VRRP statistics.

If you specify both an interface and a VRRP group, the statistics about the specified VRRP group on the specified interface are cleared; if you specify only the interface, the statistics about all the VRRP groups on the interface are cleared; if you specify neither, the statistics about all the VRRP groups on the device are cleared.

Examples

Clear the statistics about all the VRRP groups on the device.

```
<Sysname> reset vrrp statistics
```

vrrp vrid authentication-mode

Syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } *key*

undo vrrp vrid *virtual-router-id* **authentication-mode**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

simple: Plain text authentication mode.

md5: Authentication using the MD5 algorithm.

key: Authentication key, which is case sensitive.

- When **simple** authentication applies, the authentication key is in plain text with a length of 1 to 8 characters.
- When **md5** authentication applies, the authentication key is in MD5 cipher text or in plain text and the length of the key depends on its input format. If the key is input in plain text, its length is 1 to 8 characters, such as 1234567; if the key is input in cipher text, its length must be 24 characters, such as _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Description

Use the **vrrp vrid authentication-mode** command to configure authentication mode and authentication key for a VRRP group to send and receive VRRP packets.

Use the **undo vrrp vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- You may configure different authentication types and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.

Examples

Set the authentication mode and authentication key for VRRP group 1 on interface VLAN-interface 2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple Sysname
```

vrrp method

Syntax

vrrp method { **real-mac** | **virtual-mac** }

undo vrrp method

View

System view

Default Level

2: System level

Parameters

real-mac: Associates the real MAC address of the interface with the virtual IP address of the VRRP group.

virtual-mac: Associates the virtual MAC address of the switch with the virtual IP address of the VRRP group.

Description

Use the **vrrp method** command to set the mappings between the virtual IP addresses and the MAC addresses of the VRRP groups.

Use the **undo vrrp method** command to restore the default mapping.

By default, the virtual MAC address of the VRRP group is associated with the virtual IP address.

You need to configure the mapping between the virtual IP address and the MAC address before configuring a VRRP group. Otherwise, your configuration will fail.

Examples

Associate the virtual IP address of the VRRP group with the real MAC address of the interface.

```
<Sysname> system-view
[Sysname] vrrp method real-mac
```

vrrp ping-enable

Syntax

vrrp ping-enable

undo vrrp ping-enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **vrrp ping-enable** command to configure a VRRP group to respond to the ping packets destined for its virtual IP address.

Use the **undo vrrp ping-enable** command to disable a VRRP group from responding to the ping packets destined for its virtual IP address.

By default, a VRRP group responds to the ping packets destined for its virtual IP address.

Perform this configuration before configuring a VRRP group.

Examples

Configure a VRRP group to respond to the ping packets destined for its virtual IP address.

```
<Sysname> system-view
[Sysname] vrrp ping-enable
```

vrrp un-check ttl

Syntax

vrrp un-check ttl

undo vrrp un-check ttl

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **vrrp un-check ttl** command to disable TTL check on VRRP packets.

Use the **undo vrrp un-check ttl** command to enable TTL check on VRRP packets.

By default, TTL check on VRRP packets is enabled.

Examples

Disable TTL check on VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp un-check ttl
```

vrrp vrid preempt-mode

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: Virtual router ID or VRRP group number, in the range 1 to 255.

timer delay *delay-value*: Sets preemption delay. The *delay-value* argument is in the range of 0 to 255 seconds and defaults to 0 seconds.

Description

Use the **vrrp vrid preempt-mode** command to enable preemption on the switch and configure its preemption delay in the specified VRRP group.

Use the **undo vrrp vrid preempt-mode** command to disable preemption on the switch in the specified VRRP group.

Use the **undo vrrp vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

To avoid members in a VRRP group from changing their states frequently and make backups have enough time to collect information (such as routing information), each backup waits for a period of time (the preemption delay time) after it receives an advertisement with the priority lower than the local priority, then sends VRRP advertisements to start a new master election in the VRRP group and finally becomes the master.

Note that before executing the command, you need to create a VRRP group on an interface and configure the virtual IP address of the VRRP group.

Examples

Enable preemption on the switch in VRRP group 1, and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

vrrp vrid priority

Syntax

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

priority-value: Priority value of the switch in the specified VRRP group, in the range 1 to 254, A higher number indicates a higher priority.

Description

Use the **vrrp vrid priority** command to configure the priority of the switch in the specified VRRP group.

Use the **undo vrrp vrid priority** command to restore the default.

By default, the priority of a switch in a VRRP group is 100.

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- In VRRP, the role that a switch plays in a VRRP group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Examples

Set the priority of VRRP group 1 on interface VLAN-interface 2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

vrrp vrid timer advertise

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

adver-interval: Interval at which the master in the specified VRRP group sends VRRP advertisements. It ranges from 1 to 255 seconds.

Description

Use the **vrrp vrid timer advertise** command to configure the Adver_Timer of the specified VRRP group.

Use the **undo vrrp vrid timer advertise** command to restore the default.

By default the Adver_Timer is 1 second.

The Adver_Timer controls the interval at which the master sends VRRP packets.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- Switches in the same VRRP group must use the same Adver_Timer setting.

Examples

Set the master in VRRP group 1 to send VRRP advertisements at intervals of five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

vrrp vrid track

Syntax

vrrp vrid *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]

undo vrrp vrid *virtual-router-id* **track** [*track-entry-number*]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

track *track-entry-number*: Specifies a Track object to be monitored by its number. *track-entry-number* ranges from 1 to 1024.

reduced *priority-reduced*: Specifies the value by which the priority decreases. *priority-reduced* ranges from 1 to 255 and defaults to 10.

switchover: Switchover mode of a switch. If the status of the monitored Track object turns to **negative** and the switch is a backup in the VRRP group, it turns to the master immediately.

Description

Use the **vrrp vrid track** command to specify the Track object to be monitored. If the status of the monitored Track object changes to negative, the priority of the switch decreases by a specified value or the switch immediately switches to the master.

Use the **undo vrrp vrid track** command to cancel the specified Track object.

By default, no Track object is specified to be monitored.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- When the switch is the IP address owner, you cannot perform the configuration.
- When the status of the monitored Track object turns from negative to positive, the corresponding switch restores its priority automatically.

- The Track object specified in this command can be nonexistent. You can use the **vrrp vrid track** command to specify a Track object, and then create the Track object using the **track** command.

Note

For details of the Track object, refer to *Track Configuration* in the *System Volume*.

Examples

Configure to monitor Track object 1, making the priority of VRRP group 1 on VLAN-interface 2 decrease by 50 when Track object 1 turns to negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 reduced 50
```

vrrp vrid track interface

Syntax

vrrp vrid *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

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

reduced *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

Description

Use the **vrrp vrid track interface** command to configure to track the specified interface.

Use the **undo vrrp vrid track interface** command to disable tracking the specified interface.

By default, no interface is tracked.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.

Examples

On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of VRRP group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 1 reduced 50
```

vrrp vrid virtual-ip

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

virtual-address: Virtual IP address.

Description

Use the **vrrp vrid virtual-ip** command to create a VRRP group, and configure a virtual IP address for it.

Use the **undo vrrp vrid virtual-ip** command to remove an existing VRRP group or the virtual IP address of the VRRP group.

By default, no VRRP group is created.

Note that:

- The system removes a VRRP group after you delete all the virtual IP addresses in it.
- The virtual IP address of the VRRP group cannot be 0.0.0.0, 255.255.255.255, loopback address, non A/B/C address and other illegal IP addresses such as 0.0.0.1.
- Only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses can the VRRP group operate normally. If they are not in the same network segment, or the configured IP address is the network address or network broadcast address of the network segment that the interface IP address belongs to, though you can perform the configuration successfully, the state of the VRRP group is always **Initialize**, that is, VRRP does not take effect in this case.

Examples

Create VRRP group 1 and set its virtual IP address to 10.10.10.10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

Add virtual IP address 10.10.10.11 to VRRP group 1.

```
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

VRRP Configuration Commands for IPv6

display vrrp ipv6

Syntax

display vrrp ipv6 [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **display vrrp ipv6** command to display the state information of VRRP for IPv6.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both an interface and a VRRP group, only the state information of the specified VRRP group is displayed; if you only specify an interface, the state information of all the VRRP groups on the interface is displayed; if you specify neither, the state information of all the VRRP groups on the device is displayed.

Examples

Display brief information about all VRRP groups on the device for IPv6.

```
<Sysname> display vrrp ipv6
 IPv6 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Total number of virtual routers: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type        IP
 ------------------------------------------------------------------------
 Vlan100             1    Master      100     100     NONE     FE80::1
```

Display detailed information about all VRRP groups on the device.

```
<Sysname> display vrrp ipv6 verbose
 IPv6 Standby Information:
 Run Method      : VIRTUAL-MAC
```

```
Virtual IP Ping : Enable
Total number of virtual routers: 1
Interface       : Vlan-interface100
VRID            : 1                    Adver. Timer    : 100
Admin Status    : UP                   State           : Master
Config Pri      : 100                  Run Pri         : 100
Preempt Mode    : YES                  Delay Time      : 0
Auth Type       : NONE
Track IF        : Vlan200              Pri Reduced     : 10
Virtual IP      : FE80::1
Virtual MAC     : 0000-5e00-0201
Master IP       : FE80::20F:E2FF:FE49:8060
```

Table 1-3 display vrrp ipv6 command output description

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Indicates whether you can ping the virtual IPv6 address
Total number of virtual routers	Number of VRRP groups
Interface	Interface to which the VRRP group belongs
VRID	Series number of the VRRP group
Adver. Timer	VRRP advertisement interval in centiseconds
Admin Status	Administrative state: UP or DOWN
State	Status of the switch in the VRRP group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemptive mode
Delay Time	Preemption delay
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp ipv6 vrid track interface** command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the **vrrp ipv6 vrid track interface** command.
Virtual IP	Virtual IPv6 addresses of the VRRP group
Virtual MAC	Virtual MAC address corresponding to the virtual IPv6 address of the VRRP group. It is displayed only when the switch is in the state of master.
Master IP	Primary IPv6 address of the interface which belongs to the switch in the state of master

display vrrp ipv6 statistics

Syntax

display vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays VRRP statistics information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **display vrrp ipv6 statistics** command to display statistics about VRRP for IPv6.

If you specify both an interface and a VRRP group, only the statistics about the specified VRRP group are displayed; if you only specify an interface, the statistics about all the VRRP groups on the interface are displayed; if you specify neither, the statistics about all the VRRP groups on the device are displayed.

Examples

Display the statistics about all VRRP groups for IPv6.

```
<Sysname> display vrrp ipv6 statistics
 Interface              : Vlan-interface100
 VRID                   : 80
 CheckSum Errors        : 0          Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 Hop Limit Errors       : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 1          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent       : 0
 Advertise Sent         : 20

 Interface              : Vlan-interface200
 VRID                   : 10
 CheckSum Errors        : 0          Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 Hop Limit Errors       : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 1          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent       : 0
```

```
Advertise Sent          : 30

Global statistics
CheckSum Errors         : 0
Version Errors          : 0
VRID Errors             : 1439
```

Table 1-4 display vrrp ipv6 statistics command output description

Field	Description
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
Hop Limit Errors	Number of packets with hop limit errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IPv6 address list errors
Become Master	Number of times that the switch worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all VRRP groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp ipv6 statistics

Syntax

reset vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

User view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears VRRP statistics of a specific interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

Description

Use the **reset vrrp ipv6 statistics** command to clear VRRP statistics.

If you specify both an interface and a VRRP group, the statistics about the specified VRRP group on the specified interface are cleared; if you specify only an interface, the statistics about all the VRRP groups on the interface are cleared; if you specify neither, the statistics about all the VRRP groups on the device are cleared.

Examples

Clear the statistics about all the VRRP groups on the device.

```
<Sysname> reset vrrp ipv6 statistics
```

vrrp ipv6 vrid authentication-mode

Syntax

vrrp ipv6 vrid *virtual-router-id* **authentication-mode simple** *key*

undo vrrp ipv6 vrid *virtual-router-id* **authentication-mode**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

simple: Sets the authentication mode to plain text authentication.

key: Authentication key of 1 to 8 case-sensitive characters in plain text.

Description

Use the **vrrp ipv6 vrid authentication-mode** command to configure authentication mode and authentication key for the VRRP groups to send and receive VRRP packets.

Use the **undo vrrp ipv6 vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.

- You may configure different authentication types and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.

Examples

Set the authentication mode and authentication key for VRRP group 10 on interface VLAN-interface 2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 authentication-mode simple test
```

vrrp ipv6 method

Syntax

vrrp ipv6 method { **real-mac** | **virtual-mac** }

undo vrrp ipv6 method

View

System view

Default Level

2: System level

Parameters

real-mac: Associates the real MAC address of the interface with the virtual IPv6 address of the VRRP group.

virtual-mac: Associates the virtual MAC address of the switch with the virtual IPv6 address of the VRRP group.

Description

Use the **vrrp ipv6 method** command to set the mappings between the virtual IPv6 addresses and the MAC addresses of the VRRP groups.

Use the **undo vrrp ipv6 method** command to restore the default mapping.

By default, the virtual MAC address of the VRRP group is associated with the virtual IP address.

Configure the mapping between the virtual IPv6 address and the MAC address before configuring a VRRP group. Otherwise, your configuration will fail.

Examples

Associate the virtual IPv6 address of the VRRP group with the real MAC address of the interface.

```
<Sysname> system-view
[Sysname] vrrp ipv6 method real-mac
```

vrrp ipv6 ping-enable

Syntax

vrrp ipv6 ping-enable

undo vrrp ipv6 ping-enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **vrrp ipv6 ping-enable** command to configure a VRRP group to respond to the ping packets destined for its virtual IPv6 address.

Use the **undo vrrp ipv6 ping-enable** command to disable a VRRP group from responding to the ping packets destined for its virtual IPv6 address.

By default, a VRRP group responds to the ping packets destined for its virtual IPv6 address.

Perform this configuration before configuring a VRRP group.

Examples

Configure a VRRP group to respond to the ping packets destined for its virtual IPv6 address.

```
<Sysname> system-view
[Sysname] vrrp ipv6 ping-enable
```

vrrp ipv6 vrid preempt-mode

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: Virtual router ID or VRRP group number, in the range 1 to 255.

timer delay *delay-value*: Sets preemption delay. The *delay-value* argument is in the range of 0 to 255 seconds and defaults to 0 seconds.

Description

Use the **vrrp ipv6 vrid preempt-mode** command to configure preemption on the switch and configure its preemption delay in the specified VRRP group.

Use the **undo vrrp ipv6 vrid preempt-mode** command to disable preemption on the switch in the specified VRRP group.

Use the **undo vrrp ipv6 vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

If you set the switch in the VRRP group to work in non-preemptive mode, the delay period changes to zero seconds automatically.

To avoid members in a VRRP group from changing their states frequently and make backups have enough time to collect information (such as routing information), each backup waits for a period of time (the preemption delay time) after it receives an advertisement with the priority lower than the local priority, then sends VRRP advertisements to start a new master election in the VRRP group and finally becomes the master.

Note that before executing the command, you need to create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.

Examples

Enable preemption on the switch in VRRP group 80 and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 preempt-mode timer delay 5
```

vrrp ipv6 vrid priority

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

priority-value: Priority value of the switch in the specified VRRP group, in the range 1 to 254. A higher number indicates a higher priority.

Description

Use the **vrrp ipv6 vrid priority** command to configure the priority of the switch in the specified VRRP group.

Use the **undo vrrp ipv6 vrid priority** command to restore the default.

By default, the priority of a switch in a VRRP group is 100.

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- In VRRP, the role that a switch plays in a VRRP group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Examples

Set the priority of VRRP group 1 on interface VLAN-interface 2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

vrrp ipv6 vrid timer advertise

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

adver-interval: Interval at which the master in the specified VRRP group sends VRRP advertisements. It ranges from 100 to 4095 centiseconds.

Description

Use the **vrrp ipv6 vrid timer advertise** command to configure the Adver_Timer of the specified VRRP group.

Use the **undo vrrp ipv6 vrid timer advertise** command to restore the default.

By default the Adver_Timer is 100 centiseconds.

The Adver_Timer controls the interval at which the master sends VRRP packets.

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- Switches in the same VRRP group must use the same Adver_Timer setting.

Examples

Set the master in VRRP group 1 to send VRRP advertisements at intervals of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

vrrp ipv6 vrid track interface

Syntax

vrrp ipv6 vrid *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp ipv6 vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

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

reduced *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

Description

Use the **vrrp ipv6 vrid track interface** command to configure to track the specified interface.

Use the **undo vrrp ipv6 vrid track interface** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.

Examples

On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of VRRP group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 1 reduced 50
```

vrrp ipv6 vrid virtual-ip

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** *virtual-address* [**link-local**]]

View

Interface view

Default Level

2: System level

Parameters

virtual-router-id: VRRP group number, in the range 1 to 255.

virtual-address: Virtual IPv6 address.

link-local: Indicates that the virtual IPv6 address of the VRRP group is a link local address.

Description

Use the **vrrp ipv6 vrid virtual-ip** command to create a VRRP group, and configure a virtual IPv6 address for it.

Use the **undo vrrp ipv6 vrid virtual-ip** command to remove an existing VRRP group or the virtual IPv6 address of the VRRP group.

By default, no VRRP group is created.

Note that:

- The first virtual IPv6 address assigned to a VRRP group must be a link local address and only one such address is allowed in a VRRP group.
- After you remove all virtual IPv6 addresses, the VRRP group is automatically removed. The first address assigned to the group must be removed the last.

Examples

Create VRRP group 1, and configure its virtual IPv6 address as fe80::10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10
```

Configure the virtual IPv6 address of VRRP group 1 as 1::10.

```
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Table of Contents

1 HA Configuration Commands

HA Configuration Commands

display switchover state

Syntax

display switchover state [*slot-id*]

View

Any view

Default Level

1: Monitor level

Parameters

slot-id: Slot ID of the active main board (AMB) or standby main board (SMB).

Description

Use the **display switchover state** command to display the switchover state.

This command displays the switchover state on the AMB or the SMB depending on the slot number specified. The switchover state of the AMB will be displayed if no slot number is specified.

Examples

Display the switchover state on the AMB.

```
<Sysname> display switchover state
HA FSM State(master): Slave is absent.
```

Table 1-1 display switchover state command output description

Field	Description
Slave is absent	The SMB is not in the slot.
Waiting batch backup request from slave	Waiting for the backup requests from the SMB
Batch backup	Backup state
Realtime and routine backup to slave	Real-time or routine backup state

slave restart

Syntax

slave restart

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **slave restart** command to manually configure the SMB to restart.

When the backup system program operates abnormally and needs to be reloaded, you can manually restart the SMB.

Examples

Restart the SMB.

```
<Sysname> system-view
[Sysname] slave restart
The slave will reset! Continue?[Y/N]:y
```

slave switchover

Syntax

slave switchover

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **slave switchover** command to manually configure the switchover between the AMB and SMB.

Related commands: **slave switchover** { **disable** | **enable** }.

Examples

Manually configure the switchover between the AMB and the SMB.

```
<Sysname> system-view
[Sysname] slave switchover
Caution!!! Confirm switch slave to master?[Y/N] y
Starting.....
RAM Line....OK
```

slave switchover { disable | enable }

Syntax

slave switchover { **disable** | **enable** }

View

System view

Default Level

2: System level

Parameters

disable: Disables manual configuration of the switchover between the AMB and SMB.

enable: Enables manual configuration of the switchover between the AMB and SMB.

Description

Use the **slave switchover disable** command to disable manual switchover function between the AMB and SMB.

Use the **slave switchover enable** command to enable manual switchover function between the AMB and SMB.

By default, manual configuration of the switchover between the AMB and SMB is enabled.

Related commands: **slave switchover**.

Examples

Enable manual configuration of the switchover between the AMB and SMB.

```
<Sysname> system-view
[Sysname] slave switchover enable
```

Table of Contents

1 Hotfix Configuration Commands

Hotfix Configuration Commands

display patch-information

Syntax

display patch-information [**slave** | **slot** *slot-number*]

View

Any view

Default Level

3: Manage level

Parameters

slave: Displays the hotfix information on the backup main board.

slot *slot-number*: Displays the hotfix information on the specified board. *slot-number* represents the slot number of the board. The value range of this argument varies with the device model.

Description

Use the **display patch-information** command to display the hotfix information on the specified board.

If you execute this command without specifying **slave** or *slot-number*, the command is applicable to the patches on the active main board.

Examples

Display the hotfix information of the device.

```
<Sysname> display patch-information
Patch version             : PATCH-XXX001
Software version         : COMWAREV500R002B45D001
Temp patch number        : 0
Common patch number      : 2
Current patch number     : 2
Running patch number     : 0
Active patch number      : 0
Patch area length         : 0xe0000
Patch area start address: 0x18c1800
```

Table 1-1 display patch-information command output description

Field	Description
Temp patch number	Number of temporary patches
Common patch number	Number of common patches

Field	Description
Current patch number	Total number of the current patches
Running patch number	Number of running patches
Active patch number	Number of active patches

patch active

Syntax

patch active *patch-number* [**slave** | **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.

slave: Specifies the standby main board.

slot *slot-number*: Specifies a board by its slot number. The value range of this argument varies with the device model.

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.

If you execute this command without specifying **slave** or *slot-number*, the command activates the specified patches on the active main board.

Examples

Activate patch 3 and all the DEACTIVE patches before patch 3 on the standby main board.

```
<Sysname> system-view
[Sysname] patch active 3 slave
```

patch deactive

Syntax

patch deactive *patch-number* [**slave** | **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.

slave: Specifies the standby main board.

slot *slot-number*: Specifies a board by its slot number. The value range of this argument varies with the device model.

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.

If you execute this command without specifying **slave** or *slot-number*, the command deactivates the specified patches on the active main board.

Examples

Stop running patch 3 and all the ACTIVE patches after patch 3 on board 5.

```
<Sysname> system-view
[Sysname] patch deactive 3 slot 5
```

patch delete

Syntax

patch delete *patch-number* [**slave** | **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.

slave: Specifies the standby main board.

slot *slot-number*: Specifies a board by its slot number. The value range of this argument varies with the device model.

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.

If you execute this command without specifying **slave** or *slot-number*, the command deletes the specified patch(es) on the active main board.

Examples

Delete patch 3 and all the patches before patch 3 on board 5.

```
<Sysname> system-view
[Sysname] patch delete 3 slot 5
```

patch load

Syntax

patch load [**slave** | **slot** *slot-number*]

View

System view

Default Level

3: Manage level

Parameters

slave: Specifies the standby main board.

slot *slot-number*: Specifies a board by its slot number. The value range of this argument varies with the device model.

Description

Use the **patch load** command to load the patch file on the Flash to the memory patch area of the system.

The patch files of the main board, interface board, and L3+ board are **patchmain**, **patchio**, and **patchl3plus** respectively.

The active main board and the standby main board load their patch files from their own Flash. The administrator needs to ensure the consistency of the patch files on the active and standby main boards.

If you execute this command without specifying **slave** or *slot-number*, the command loads the patch file to the active main board.

Examples

Load the patch file for board 3.

```
<Sysname> system-view
[Sysname] patch load slot 3
```

patch run

Syntax

patch run *patch-number* [**slave** | **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.

slave: Specifies the standby main board.

slot *slot-number*: Specifies a board by its slot number. The value range of this argument varies with the device model.

Description

Use the **patch run** command to confirm the running of the specified patch and all the ACTIVE patches before the specified patch number.

This operation is applicable to patches in the ACTIVE state only.

If the running of a patch is confirmed, after the system reboots, the original ACTIVE patches are still ACTIVE and take effect.

If you execute this command without specifying **slave** or *slot-number*, the command confirms the running of the specified patch(es) on the active main board.

Examples

Confirm the running of patch 3 and all the ACTIVE patches before patch 3 on board 5.

```
<Sysname> system-view
[Sysname] patch run 3 slot 5
```