H3C Access Controllers

Network Connectivity Command Reference

New H3C Technologies Co., Ltd.
http://www.h3c.com

Document version: 6W100-20220530
Product version: R5447P04

Copyright © 2022, New H3C Technologies Co., Ltd. and its licensors

All rights reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of New H3C Technologies Co., Ltd.

Trademarks

Except for the trademarks of New H3C Technologies Co., Ltd., any trademarks that may be mentioned in this document are the property of their respective owners.

Notice

The information in this document is subject to change without notice. All contents in this document, including statements, information, and recommendations, are believed to be accurate, but they are presented without warranty of any kind, express or implied. H3C shall not be liable for technical or editorial errors or omissions contained herein.

Preface

This command reference describes the network connectivity configuration commands.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.
- Documentation feedback.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the H3C access controllers.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) 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 opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

MAC address table commands ····· 1

display mac-address ····· 1
display mac-address aging-time ····· 2
display mac-address mac-learning ····· 3
display mac-address mac-move ····· 3
mac-address (interface view) ····· 5
mac-address (system view) ····· 6
mac-address mac-learning enable ····· 7
mac-address mac-learning priority ····· 8
mac-address max-mac-count ····· 9
mac-address max-mac-count enable-forwarding ····· 11
mac-address notification mac-move ····· 12
mac-address notification mac-move suppression (interface view) ····· 13
mac-address notification mac-move suppression (system view) ····· 14
mac-address timer ····· 15
snmp-agent trap enable mac-address ····· 17

MAC address table commands

This document covers the configuration of unicast MAC address entries, including static, dynamic, and blackhole MAC address entries.

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

display mac-address

Use **display mac-address** to display MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

dynamic: Displays dynamic MAC address entries.

static: Displays static MAC address entries.

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

blackhole: Displays blackhole MAC address entries.

count: Displays only the number of MAC address entries that match all entry attributes you specify in the command. Detailed information about MAC address entries is not displayed. For example, you can use the **display mac-address vlan 20 dynamic count** command to display the number of dynamic entries for VLAN 20. If you do not specify an entry attribute, the command displays the number of entries in the MAC address table. If you do not specify this keyword, the command displays detailed information about the specified MAC address entries.

Usage guidelines

Use this command to display static, dynamic, or blackhole MAC address entries. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID.

If you do not specify any parameters, the command displays all MAC address entries.

This command displays dynamic MAC address entries for an aggregate interface only when the aggregate interface has a minimum of one Selected member port.

Examples

Display MAC address entries for VLAN 100.

```
<Sysname> display mac-address vlan 100
MAC Address      VLAN ID    State           Port/Nickname           Aging
0033-0033-0033   100        Blackhole       N/A                     N
0000-0000-0002   100        Static          GE1/0/1                 N
00e0-fc00-5829   100        Learned         GE1/0/2                 Y
```

Display the number of MAC address entries.

```
<Sysname> display mac-address count
1 mac address(es) found.
```

Table 1 Command output

Field	Description
VLAN ID	ID of the VLAN to which the outgoing interface of the MAC address entry belongs.
State	MAC address entry state: • **Static**—Static MAC address entry. • **Learned**—Dynamic MAC address entry. Dynamic entries can be learned or manually configured. • **Blackhole**—Blackhole MAC address entry.
Port/Nickname	When the field displays an interface name, the field indicates the outgoing interface for packets that are destined for the MAC address. This field displays **N/A** for a blackhole MAC address entry. The **Nickname** field is not supported in the current software version.
Aging	Whether the entry can age out: • **Y**—The entry can age out. • **N**—The entry never ages out.
mac address(es) found	Number of matching MAC address entries.

Related commands

mac-address

mac-address timer

display mac-address aging-time

Use **display mac-address aging-time** to display the aging timer for dynamic MAC address entries.

Syntax

display mac-address aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging timer for dynamic MAC address entries.

```
<Sysname> display mac-address aging-time
```

```
MAC address aging time: 300s.
```

Related commands

mac-address timer

display mac-address mac-learning

Use **display mac-address mac-learning** to display the global MAC address learning status and the MAC learning status of the specified interface or all interfaces.

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the global MAC address learning status and the MAC address learning status of all interfaces.

Examples

Display the global MAC address learning status and the MAC learning status of all interfaces.

```
<Sysname> display mac-address mac-learning
Global MAC address learning status: Enabled.

Port                          Learning Status
GE1/0/1                       Enabled
GE1/0/2                       Enabled
```

Table 2 Command output

Field	Description
Global MAC address learning status	Global MAC address learning status: • Enabled. • Disabled.
Learning Status	MAC address learning status of an interface: • Enabled. • Disabled.

Related commands

mac-address mac-learning enable

display mac-address mac-move

Use **display mac-address mac-move** to display the MAC address move records after the device is started.

Syntax

In standalone mode:

display mac-address mac-move

In IRF mode:

display mac-address mac-move [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays MAC address move records for all IRF member devices. (In IRF mode.)

Usage guidelines

When a MAC address frequently moves between the specified two interfaces, Layer 2 loops might occur in the network. To discover and locate loops, you can view the MAC address move records.

In the MAC address move records, records with the same MAC address, VLAN, source port, and current port are considered to be one record.

(In standalone mode.) A device can save a maximum of 20 MAC address move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time.

(In IRF mode.) An IRF member device can save a maximum of 20 MAC address move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time.

Examples

Display the MAC address move records for a slot.

```
<Sysname> display mac-address mac-move slot 1
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 1
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:30 1
---  2 MAC address moving records found  ---
```

Display the MAC address move records.

```
<Sysname> display mac-address mac-move
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 1
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:30 1
0000-0094-0001 1    GE1/0/3       GE1/0/4       2013-05-20 13:42:22 13
0000-0094-0001 1    GE1/0/4       GE1/0/3       2013-05-20 13:42:21 12
---  4 MAC address moving records found  ---
```

Table 3 Command output

Field	Description
VLAN	VLAN to which the outgoing interface of the MAC address entry

Field	Description
	belongs.
Current port	Interface to which the MAC address was moved.
Source port	Interface from which the MAC address was moved.
Last time	Last time when the MAC address was moved.
Times	Number of MAC address moves after the device is started. For a MAC address record, the number of MAC address moves is increased by 1 when a new MAC address move has the same **MAC address**, **VLAN**, **Current Port**, and **Source Port** fields as the MAC address record.

Related commands

mac-address notification mac-move

mac-address (interface view)

Use **mac-address** to add or modify a MAC address entry on an interface.

Use **undo mac-address** to delete a MAC address entry on an interface.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

Default

An interface is not configured with MAC address entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the specified interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Typically, the device automatically builds the MAC address table by learning the source MAC addresses of incoming frames on each interface. However, you can manually configure static MAC address entries. For a MAC address, a manually configured static entry takes precedence over a dynamically learned entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101 on GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Add a static entry for MAC address 000f-e201-0101 on Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

Related commands

display mac-address

mac-address (system view)

mac-address (system view)

Use **mac-address** to add or modify a MAC address entry.

Use **undo mac-address** to delete one or all MAC address entries.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **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**] **interface** *interface-type interface-number*

undo mac-address [[*mac-address*] **vlan** *vlan-id*]

Default

The system is not configured with MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

blackhole: Specifies blackhole MAC address entries. Packets whose source or destination MAC addresses match blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

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

Usage guidelines

You can use this command to configure the following types of MAC address entries:

- Dynamic entries.

  Dynamic entries include manually configured dynamic entries and automatically learned dynamic entries.

- Static entries.

  For a MAC address, a manually configured static entry takes precedence over a dynamic entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

- Blackhole entries.

  To drop frames with the specified source MAC addresses or destination MAC addresses, you can configure blackhole entries.

A static or blackhole entry can overwrite a dynamic entry, but not vice versa.

If you execute the **undo mac-address** command without specifying any parameters, this command deletes all unicast MAC address entries and static multicast MAC address entries.

You can delete all the MAC address entries (including unicast and static multicast MAC address entries) from the specified VLAN. You can also delete only one type (dynamic, static, or blackhole) of MAC address entries.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

Related commands

display mac-address

mac-address (interface view)

mac-address mac-learning enable

Use **mac-address mac-learning enable** to enable MAC address learning on an interface.

Use **undo mac-address mac-learning enable** to disable MAC address learning on an interface.

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

Default

MAC address learning is enabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

To prevent the MAC address table from becoming saturated, you can disable MAC address learning.

For example, a number of packets with different source MAC addresses reaching a device can affect the MAC address table update. To avoid such attacks, you can disable MAC address learning by following these guidelines:

- You can disable MAC address learning on a per-interface basis. If you disable MAC address learning globally, MAC address learning is disabled for all interfaces. The device then stops learning MAC addresses and cannot dynamically update the MAC address table.
- Because disabling MAC address learning can result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on an interface. For more information about broadcast storm suppression, see *Interface Configuration Guide*.
- With MAC address learning enabled globally, you can disable MAC address learning for an interface or VLAN.
- After MAC address learning is disabled, existing dynamic MAC address entries can age out.

Examples

Disable MAC address learning globally.

```
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
```

Disable MAC address learning on GigabitEthernet 1/0/1.

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

Disable MAC address learning on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo mac-address mac-learning enable
```

Related commands

display mac-address mac-learning

mac-address mac-learning priority

Use **mac-address mac-learning priority** to assign MAC learning priority to an interface.

Use **undo mac-address mac-learning priority** to restore the default.

Syntax

mac-address mac-learning priority { **high** | **low** }

undo mac-address mac-learning priority

Default

Low MAC address learning priority is used.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

high: Assigns high MAC learning priority.

low: Assigns low MAC learning priority.

Usage guidelines

The MAC address learning priority values can be high and low. An interface with high MAC address learning priority can learn any MAC address. An interface with low MAC address learning priority can learn only the MAC addresses that have not been learned by high-priority interfaces.

The MAC learning priority mechanism can help defend your network against MAC address spoofing attacks. To prevent the downlink interface from learning the MAC address of an upper layer device (for example, the gateway), you can perform the following tasks:

- Assign high MAC learning priority to an uplink interface.
- Assign low MAC learning priority to a downlink interface.

Examples

Assign high MAC learning priority to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address mac-learning priority high
```

Assign high MAC learning priority to Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address mac-learning priority high
```

mac-address max-mac-count

Use **mac-address max-mac-count** to set the MAC learning limit on an interface.

Use **undo mac-address max-mac-count** to restore the default.

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

Default

The MAC learning limit on an interface is equal to the maximum value of the *count* argument.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

count: Specifies the maximum number of MAC addresses that can be learned on an interface. When the argument is set to 0, the interface is not allowed to learn MAC addresses.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	0 to 512
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2510H: 0 to 2048 WX2510-F: 0 to 2048 WX2508H-PWR-LTE: 0 to 2048 WX2540H: 0 to 3072 WX2540H-F: 0 to 3072 WX2560H: 0 to 6144
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	0 to 6144
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	WX3010H-X: 0 to 3072 WX3010H-L: 0 to 2048 WX3010H: 0 to 4096 WX3024H-L: 0 to 4096 WX3024H: 0 to 8192 WX3024H-F: 0 to 8192
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: 0 to 4096 WX3510H: 0 to 8192 WX3520H: 0 to 16384 WX3520H-F: 0 to 16384 WX3540H: 0 to 20480
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 0 to 10240 WX5540E: 0 to 30720
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	WX5540H: 0 to 30720 WX5560H: 0 to 40960 WX5580H: 0 to 49152
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX20: 0 to 20480 LSUM1WCMX20RT: 0 to 20480 EWPXM2WCMD0F: 0 to 20480 LSUM1WCME0: 0 to 30720 EWPXM1WCME0: 0 to 30720 LSQM1WCMX40: 0 to 30720 LSUM1WCMX40RT: 0 to

Hardware series	Model	Product code	Value range
			30720 EWPXM1MAC0F: 0 to 30720

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	WX1804H: 0 to 512 WX1810H: 0 to 2048 WX1820H: 0 to 2048 WX1840H: 0 to 2560
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	WX3820H: 0 to 16384 WX3840H: 0 to 20480
WX5800H series	WX5860H	EWP-WX5860H-GL	0 to 40960

Usage guidelines

This command helps limit the MAC address table size. When the number of MAC address entries learned by an interface reaches the limit, the interface stops learning MAC address entries.

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 200 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
```

Related commands

mac-address

mac-address max-mac-count enable-forwarding (interface view)

mac-address max-mac-count enable-forwarding

Use **mac-address max-mac-count enable-forwarding** to enable the device to forward unknown frames received on an interface after the MAC learning limit on the interface is reached. Unknown frames refer to frames whose source MAC addresses are not in the MAC address table.

Use **undo mac-address max-mac-count enable-forwarding** to disable the device from forwarding unknown frames received on an interface after the MAC learning limit on the interface is reached.

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

Default

When the MAC learning limit on an interface is reached, the device can forward unknown frames received on the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 200 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
```

Disable the device from forwarding unknown frames received on GigabitEthernet 1/0/1 after the MAC learning limit on GigabitEthernet 1/0/1 is reached.

```
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

Related commands

mac-address

mac-address max-mac-count

mac-address notification mac-move

Use **mac-address notification mac-move** to enable MAC address move notifications and optionally specify a MAC move detection interval.

Use **undo mac-address notification mac-move** to disable MAC address move notifications.

Syntax

mac-address notification mac-move [**interval** *interval*]

undo mac-address notification mac-move

Default

MAC address move notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for detecting MAC address moves, in the range of 1 to 60 minutes. If you do not specify this option, the default setting of 1 minute is used.

Usage guidelines

With MAC address move notifications enabled, the system records the MAC address move logs every MAC move detection interval. Each record of the MAC address move logs contains the following information:

- MAC address.
- VLAN ID of the MAC address entry.
- Current port and source port of the MAC address moves.
- Number of MAC address moves within a detection interval.

A MAC address can have only one MAC address move record. If a MAC address moves multiple times, the new record overrides the old record.

(In standalone mode.) Within a detection interval, the device can record MAC address move information for a maximum of 20 MAC addresses. If the limit is reached, the device only updates existing records, and new MAC address moves are not recorded. Then in the next detection interval, a new MAC address move record will overwrite the earliest one generated in the previous detection interval.

(In IRF mode.) Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. If the limit is reached, the device only updates existing records, and new MAC address moves are not recorded. Then in the next detection interval, a new MAC address move record will overwrite the earliest one generated in the previous detection interval.

After you execute this command, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move notifications.

```
<Sysname> system-view
[Sysname] mac-address notification mac-move
[Sysname]
%May 14 17:16:45:688 2013 Sysname MAC/4/MAC_FLAPPING: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

The output shows that:

- The VLAN ID of MAC address 0000-0012-0034 is VLAN 500.
- The MAC address moved from GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2.
- The MAC address has moved once within a MAC move detection interval.

Related commands

display mac-address mac-move

mac-address notification mac-move suppression (interface view)

Use **mac-address notification mac-move suppression** to enable MAC address move suppression on an interface.

Use **undo mac-address notification mac-move suppression** to disable MAC address move suppression on an interface.

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

Default

MAC address moves are not suppressed.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This feature shuts an interface down when a MAC address has been moved to or from the interface more than the suppression threshold within a MAC move detection interval. The shutdown interface automatically goes up after a suppression interval. Also, you can use the **shutdown** command and then the **undo shutdown** command to bring up the interface.

When MAC address move suppression shuts an interface down, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move suppression on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address notification mac-move suppression
```

Related commands

mac-address notification mac-move suppression (system view)

mac-address notification mac-move suppression (system view)

Use **mac-address notification mac-move suppression** to set the suppression interval or the suppression threshold.

Use **undo mac-address notification mac-move suppression** to restore the default.

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

Default

The suppression interval is 30 seconds. The suppression threshold is 3.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the MAC address move suppression interval during which a suppressed interface stays down. The value range for the *interval-value* argument is 30 to 86400 seconds. If you do not specify this option, the default suppression interval of 30 seconds is used.

threshold *threshold*: Specifies the suppression threshold for MAC address moves sourced from or destined for an interface within a MAC move detection interval. The value range for this argument is 0 to 1024. If you do not specify this option, the default suppression threshold of 3 is used.

Usage guidelines

For this command to take effect on an interface, you must also enable MAC address move suppression on the interface.

If you set the suppression interval or suppression threshold multiple times, the most recent configuration applies. The suppression interval setting is independent of the suppression threshold setting.

Examples

Set the suppression interval to 40 seconds and the suppression threshold to 1 for MAC address moves.

```
<Sysname> system-view
[Sysname] mac-address notification mac-move suppression interval 40
[Sysname] mac-address notification mac-move suppression threshold 1
```

Related commands

mac-address notification mac-move suppression (interface view)

mac-address timer

Use **mac-address timer** to set the aging timer for dynamic MAC address entries.

Use **undo mac-address timer** to restore the default.

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

Default

The aging timer is 300 seconds for dynamic MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

aging *seconds*: Specifies an aging timer for dynamic MAC address entries, in seconds.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	10 to 1400
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2510H: 10 to 630 WX2510-F: 10 to 630 WX2508H-PWR-LTE: 10 to 1400 WX2540H: 10 to 630 WX2540H-F: 10 to 630 WX2560H: 10 to 630
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	10 to 630
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR	WX3010H-X: 100 to 1400 WX3010H-L: 100 to 1400 WX3010H: 100 to 1400

Hardware series	Model	Product code	Value range
	WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	WX3024H-L: 100 to 1400 WX3024H: 100 to 1400 WX3024H-F: 100 to 1400
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: 10 to 630 WX3510H: 100 to 1400 WX3520H: 100 to 1400 WX3520H-F: 100 to 1400 WX3540H: 100 to 1400
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 100 to 1400 WX5540E: 100 to 1400
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	WX5540H: 100 to 1400 WX5560H: 100 to 1400 WX5580H: 100 to 1400
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX20: 100 to 1400 LSUM1WCMX20RT: 100 to 1400 EWPXM2WCMD0F: 100 to 1400 LSUM1WCME0: 10 to 1400 EWPXM1WCME0: 10 to 1400 LSQM1WCMX40: 100 to 1400 LSUM1WCMX40RT: 100 to 1400 EWPXM1MAC0F: 100 to 1400

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	WX1804H: 10 to 1400 WX1810H: 10 to 1400 WX1820H: 10 to 1400 WX1840H: 10 to 1400
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	WX3820H: 100 to 1400 WX3840H: 100 to 1400
WX5800H series	WX5860H	EWP-WX5860H-GL	100 to 1400

`no-aging`: Configures dynamic MAC address entries not to age.

Usage guidelines

To set the aging timer appropriately, follow these guidelines:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.

- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

Examples

Set the aging time to 500 seconds for dynamic MAC address entries.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

Related commands

display mac-address aging-time

snmp-agent trap enable mac-address

Use **snmp-agent trap enable mac-address** to enable SNMP notifications for the MAC address table.

Use **undo snmp-agent trap enable mac-address** to disable SNMP notifications for the MAC address table.

Syntax

snmp-agent trap enable mac-address [**mac-move**]

undo snmp-agent trap enable mac-address [**mac-move**]

Default

SNMP notifications are enabled for the MAC address table.

Views

System view

Predefined user roles

network-admin

Parameters

mac-move: Specifies notifications about the MAC address moves for the MAC address table. If you do not specify this keyword, the command enables all types of SNMP notifications for the MAC address table.

Usage guidelines

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For information about SNMP and information center configuration, see *Network Management and Monitoring Configuration Guide* and *System Management Configuration Guide*, respectively.

The MAC address table supports only SNMP notifications about MAC address moves. When you enable or disable SNMP notifications about MAC address moves, you enable or disable all types of SNMP notifications for the MAC address table.

Examples

Disable SNMP notifications about MAC address moves for the MAC address table.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable mac-address mac-move
```

Related commands

`mac-address notification mac-move`

Contents

Ethernet link aggregation commands 1

bandwidth 1
default 1
description 2
display interface 2
display lacp system-id 5
display link-aggregation load-sharing mode 6
display link-aggregation member-port 7
display link-aggregation summary 9
display link-aggregation verbose 10
interface bridge-aggregation 13
jumboframe enable 15
lacp edge-port 16
lacp mode 17
lacp period short 18
lacp system-priority 18
link-aggregation global load-sharing mode 19
link-aggregation ignore vlan 19
link-aggregation lacp traffic-redirect-notification enable 20
link-aggregation load-sharing mode 21
link-aggregation load-sharing mode local-first 22
link-aggregation mode 23
link-aggregation port-priority 24
link-aggregation selected-port maximum 25
link-aggregation selected-port minimum 27
port link-aggregation group 29
reset counters interface 31
reset lacp statistics 31
shutdown 32

Ethernet link aggregation commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] bandwidth 10000
```

default

Use **default** to restore the default settings for an aggregate interface.

Syntax

default

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

△ **CAUTION:**

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Layer 2 aggregate interface 1.

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

description

Use **description** to configure the description of an interface.

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

Syntax

description *text*

undo description

Default

The description of an interface is *interface-name* **Interface**. For example, the default description of Bridge-Aggregation 1 is **Bridge-Aggregation1 Interface**.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **connect to the lab** for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description connect to the lab
```

display interface

Use **display interface** to display aggregate interface information.

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you specify an aggregate interface type but do not specify an interface number, the command displays information about all aggregate interfaces of the specified type.

Examples

Display detailed information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1
Bridge-Aggregation1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
  Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
  Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
  Input (total):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
  Input (normal):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
  Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, - aborts
          - ignored, - parity errors
  Output (total): 1042508 packets, 133441832 bytes
          1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
  Output (normal): 1042508 packets, 133441832 bytes
          1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
  Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
```

```
          - lost carrier, - no carrier
```

Display brief information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                UP   auto    A      A    1
```

Table 1 Command output

Field	Description
Bridge-Aggregation1	Layer 2 aggregate interface name.
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
IP packet frame type	IPv4 packet framing format.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the bandwidth is 0 kbps.
Unknown-speed mode, unknown-duplex mode	The interface speed and duplex mode are unknown.
Port link-type	Port link type: • Access. • Trunk. • Hybrid.
Tagged VLANs	VLAN whose packets are sent out of this interface with a tag.
Untagged VLANs	VLAN whose packets are sent out of this interface without a tag.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 seconds input/output rate	Average input or output rate over the last 300 seconds.
Input/Output (total)	Statistics of all packets received or sent on the interface.
Input/Output (normal)	Statistics of all normal packets received or sent on the interface.
Brief information on interfaces in bridge mode	Brief information about Layer 2 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down.

Field	Description
	• **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.

display lacp system-id

Use **display lacp system-id** to display the local system ID.

Syntax

display lacp system-id

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

You can use the **lacp system-priority** command to change the LACP priority of the local system. The LACP priority value is specified in decimal format in the **lacp system-priority** command. However, it is displayed in hexadecimal format in the output from the **display lacp system-id** command.

Examples

Display the local system ID.

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

Table 2 Command output

Field	Description
Actor System ID: 0x8000, 0000-fc00-6504	Local system ID, which contains the system LACP priority (0x8000 in this sample output) and the system MAC address (0000-FC00-6504 in this sample output).

Related commands

lacp system-priority

display link-aggregation load-sharing mode

Use **display link-aggregation load-sharing mode** to display global or group-specific link-aggregation load sharing modes.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the global link-aggregation load sharing modes.

If you specify the **interface** keyword, but do not specify an interface, the command displays all group-specific load sharing modes.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

Examples

Display the global link-aggregation load sharing mode. This example displays the default setting.

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
```

Display the global link-aggregation load sharing mode. This example displays a user-configured setting.

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 1. This example displays the default setting.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
```

```
Bridge-Aggregation1 load-sharing mode:
Layer 2 traffic: packet type-based sharing
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 1. This example displays a user-configured setting.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

Table 3 Command output

Field	Description
Link-aggregation load-sharing mode	Global link-aggregation load sharing mode. By default, this field displays the link-aggregation load sharing mode for Layer 2 traffic. If you have configured the global link-aggregation load sharing mode, this field displays the configured mode.
Bridge-Aggregation1 load-sharing mode	Link-aggregation load sharing mode of Layer 2 aggregation group 1. By default, this field displays the global link-aggregation load sharing modes. If you have configured a link-aggregation load sharing mode for this aggregation group, this field displays the configured mode.
Layer 2 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, Layer 2 traffic is load shared based on the packet type.
destination-mac address, source-mac address	User-configured link-aggregation load sharing mode. In this sample output, traffic is load shared based on source and destination MAC addresses.

display link-aggregation member-port

Use **display link-aggregation member-port** to display detailed link aggregation information about the specified member ports.

Syntax

display link-aggregation member-port [*interface-list*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

A member port in a static aggregation group cannot obtain information about the peer group. For such member ports, the command displays the port number, port priority, and operational key of only the local end.

Examples

Display detailed information about GigabitEthernet 1/0/1, which is a member port of a static aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

Display detailed information about GigabitEthernet 1/0/2, which is a member port of a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation2
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 4 Command output

Field	Description
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout

Field	Description
	interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Aggregate interface to which the member port belongs.
Local	Information about the local end.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the peer end.
System ID	Peer system ID, containing the system LACP priority and the system MAC address.
Received LACP Packets	Total number of LACP packets received.
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

display link-aggregation summary

Use **display link-aggregation summary** to display brief information about all aggregation groups.

Syntax

display link-aggregation summary

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Static link aggregation groups cannot obtain information about the peer groups. As a result, the **Partner ID** field displays **None** or nothing for a static link aggregation group.

Examples

Display brief information about all aggregation groups.

```
<Sysname> display link-aggregation summary
Aggregate Interface Type:
BAGG -- Bridge-Aggregation, BLAGG –- Blade-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             Selected  Unselected  Individual  Share
Interface  Mode                         Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
BAGG2      S     0x8000,00e0-fcff-ff01  2         0           0           Shar
```

Table 5 Command output

Field	Description
Aggregate Interface Type	Aggregate interface type: **BAGG**—Layer 2.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Actor System ID	Local system ID, which contains the local system LACP priority and the local system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the peer system, which contains the peer system LACP priority and the peer system MAC address.
Selected Ports	Total number of Selected ports.
Unselected Ports	Total number of Unselected ports.
Individual Ports	Total number of Individual ports.
Share Type	Load sharing type.

display link-aggregation verbose

Use **display link-aggregation verbose** to display detailed information about the aggregation groups that correspond to the specified aggregate interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

Usage guidelines

If you do not specify an aggregate interface type, the command displays detailed information about all aggregation groups.

If you specify an aggregate interface type but do not specify an interface number, the command displays detailed information about all aggregation groups of the specified type.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

Examples

Display detailed information about Layer 2 aggregation group 1, which is a dynamic aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/2          S       32768    2         {ACDEF}
  GE1/0/3          S       32768    2         {ACDEF}
  GE1/0/4          S       32768    2         {AG}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/2          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/4          1       32768    2         0x8000, 0000-0000-0000 {DEF}
```

Display detailed information about Layer 2 aggregation group 1, which is a static aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
  GE1/0/4          S       32768    1
```

Table 6 Command output

Field	Description
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Port Status	Port state: • **Selected**. • **Unselected**. • **Individual**.
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Name of the aggregate interface.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
System ID	Local system ID, containing the local system LACP priority and the local system MAC address.
Local	Information about the local end: • **Port**—Port type and number. • **Status**—Port state, which can be Selected, Unselected, or Individual. • **Priority**—Port priority. • **Oper-Key**—Operational key. • **Flag**—LACP state flag. **NOTE:** For static aggregation groups, the **Flag** field is not displayed.
Remote	Information about the peer end:

Field	Description
	• **Actor**—Type and number of the local port. This field displays the **(R)** flag next to the port if its peer port is the reference port. • **Partner**—Index of the peer port. • **Priority**—Priority of the peer port. • **Oper-Key**—Operational key of the peer port. • **System ID**—System ID of the peer end. • **Flag**—LACP state flag of the peer end.

interface bridge-aggregation

Use **interface bridge-aggregation** to create a Layer 2 aggregate interface and enter its view, or enter the view of an existing Layer 2 aggregate interface.

Use **undo interface bridge-aggregation** to delete a Layer 2 aggregate interface.

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

Default

No Layer 2 aggregate interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a Layer 2 aggregate interface number.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX2560H-PWR	EWP-WX1804H-PWR-CN	Fixed at 1
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Fixed at 1
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Fixed at 1
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	1 and 2

Hardware series	Model	Product code	Value range
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: Fixed at 1 WX3510H: 1 to 4 WX3520H: 1 to 4 WX3520H-F: 1 to 4 WX3540H: 1 to 4
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 1 to 4 WX5540E: 1 to 6
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	1 to 6
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Fixed at 1

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Fixed at 1
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	1 to 4
WX5800H series	WX5860H	EWP-WX5860H-GL	1 to 6

Usage guidelines

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number. The aggregation group operates in static aggregation mode by default.

Deleting a Layer 2 aggregate interface also deletes 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, and enter its view.

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

jumboframe enable

Use **jumboframe enable** to allow the jumbo frames on an interface to pass through.

Use **undo jumboframe enable** to deny jumbo frames on an interface.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

An aggregate interface allows jumbo frames with a maximum length of 4000 bytes to pass through.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum length of jumbo frames, in bytes.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	1700 to 4000
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	1700 to 4000
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	1700 to 4000
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	1700 to 4000
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	1700 to 4000

Hardware series	Model	Product code	Value range
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	1700 to 4000
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	1700 to 3996
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	1700 to 4000

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	1700 to 4000
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	1700 to 3996
WX5800H series	WX5860H	EWP-WX5860H-GL	1700 to 3996

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames to pass through on Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] jumboframe enable
```

lacp edge-port

Use **lacp edge-port** to configure an aggregate interface as an edge aggregate interface.

Use **undo lacp edge-port** to restore the default.

Syntax

lacp edge-port

undo lacp edge-port

Default

An aggregate interface does not operate as an edge aggregate interface.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Use this command on the aggregate interface that connects the device to a server if dynamic link aggregation is configured only on the device. This feature improves link reliability by enabling all member ports of the aggregation group to forward packets.

This command takes effect only on an aggregate interface corresponding to a dynamic aggregation group.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Examples

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lacp edge-port
```

lacp mode

Use **lacp mode passive** to configure LACP to operate in passive mode on a port.

Use **undo lacp mode** to restore the default.

Syntax

lacp mode passive

undo lacp mode

Default

LACP operates in active mode on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on member ports of dynamic aggregation groups.

When LACP is operating in passive mode on a local member port and its peer port, both ports cannot send LACPDUs. When LACP is operating in active mode on either end of a link, both ports can send LACPDUs.

Examples

Configure LACP to operate in passive mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

lacp period short

Use **lacp period short** to enable the short LACP timeout interval (3 seconds) on an interface.

Use **undo lacp period** to restore the default.

Syntax

lacp period short

undo lacp period

Default

The LACP timeout interval is the long timeout interval (90 seconds) on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable the short LACP timeout interval (3 seconds) on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

lacp system-priority

Use **lacp system-priority** to set the system LACP priority.

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

Syntax

lacp system-priority *priority*

undo lacp system-priority

Default

The system LACP priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority: Specifies the system LACP priority in the range of 0 to 65535. The smaller the value, the higher the system LACP priority.

Examples

Set the system LACP priority to 64.

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

Related commands

link-aggregation port-priority

link-aggregation global load-sharing mode

Use **link-aggregation global load-sharing mode** to set the global link-aggregation load sharing mode.

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

Syntax

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

undo link-aggregation global load-sharing mode

Default

Link aggregation groups distribute traffic based on source and destination IP addresses.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

Examples

Set the global load sharing mode to load share packets based on destination MAC addresses.

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

Related commands

link-aggregation load-sharing mode

link-aggregation ignore vlan

Use **link-aggregation ignore vlan** to configure a Layer 2 aggregate interface to ignore the specified VLANs.

Use **undo link-aggregation ignore vlan** to remove the specified ignored VLANs for a Layer 2 aggregate interface.

Syntax

link-aggregation ignore vlan *vlan-id-list*

undo link-aggregation ignore vlan *vlan-id-list*

Default

A Layer 2 aggregate interface does not ignore any VLANs.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command takes effect only when the link type of the Layer 2 aggregate interface is hybrid or trunk.

With this command configured, a Layer 2 aggregate interface ignores the permitted VLAN and VLAN tagging mode configuration of the specified VLANs when choosing Selected ports.

Examples

Configure Layer 2 aggregate interface **bridge-aggregation 1** to ignore VLAN 50.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation ignore vlan 50
```

link-aggregation lacp traffic-redirect-notification enable

Use **link-aggregation lacp traffic-redirect-notification enable** to enable link-aggregation traffic redirection.

Use **undo link-aggregation lacp traffic-redirect-notification enable** to disable link-aggregation traffic redirection.

Syntax

link-aggregation lacp traffic-redirect-notification enable

undo link-aggregation lacp traffic-redirect-notification enable

Default

Link-aggregation traffic redirection is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature redirects traffic on a Selected port to the remaining available Selected ports of an aggregation group if the port is shut down by using the **shutdown** command or the slot that hosts the port reboots.

NOTE:

The device does not redirect traffic to member ports that become Selected during the traffic redirection process.

This feature ensures zero packet loss for known unicast traffic, but does not protect unknown unicast traffic.

This feature applies only to dynamic link aggregation groups.

To prevent traffic interruption, enable link-aggregation traffic redirection on devices at both ends of the aggregate link.

To prevent packet loss that might occur when a slot reboots, do not enable spanning tree together with link-aggregation traffic redirection.

Examples

Enable link-aggregation traffic redirection.

```
<Sysname> system-view
[Sysname] link-aggregation lacp traffic-redirect-notification enable
```

link-aggregation load-sharing mode

Use **link-aggregation load-sharing mode** to set the link-aggregation load sharing mode for an aggregation group.

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

Syntax

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

undo link-aggregation load-sharing mode

Default

An aggregation group uses the global link-aggregation load sharing mode.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

Examples

Configure Layer 2 aggregation group 1 to load share packets based on destination MAC addresses.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation load-sharing mode destination-mac
```

Related commands

link-aggregation global load-sharing mode

link-aggregation load-sharing mode local-first

Use **link-aggregation load-sharing mode local-first** to enable local-first load sharing for link aggregation.

Use **undo link-aggregation load-sharing mode local-first** to disable local-first load sharing for link aggregation.

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	No
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	No
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes

Hardware series	Model	Product code	Command compatibility
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Yes

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	No
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

Default

Local-first load sharing is enabled for link aggregation.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use local-first load sharing in a multidevice link aggregation scenario to distribute traffic preferentially across member ports on the ingress card or device.

If you disable local-first load sharing, packets of an aggregate interface are load shared among all Selected ports on IRF member devices.

Examples

Disable local-first load sharing for link aggregation.

```
<Sysname> system-view
[Sysname] undo link-aggregation load-sharing mode local-first
```

link-aggregation mode

Use **`link-aggregation mode dynamic`** to configure an aggregation group to operate in dynamic aggregation mode and enable LACP.

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

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

Default

An aggregation group operates in static aggregation mode.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Aggregation mode change might cause Selected member ports to become Unselected.

When you change the aggregation mode, make sure you understand the impact of the change on services.

Examples

Configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

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

link-aggregation port-priority

Use **link-aggregation port-priority** to set the port priority of an interface.

Use **undo link-aggregation port-priority** to restore the default.

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

Default

The port priority of an interface is 32768.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority: Specifies the port priority in the range of 0 to 65535. The smaller the value, the higher the port priority.

Examples

Set the port priority to 64 for Layer 2 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-aggregation port-priority 64
```

Related commands

lacp system-priority

link-aggregation selected-port maximum

Use **link-aggregation selected-port maximum** to set the maximum number of Selected ports allowed in an aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default.

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

Default

The maximum number of Selected ports allowed in an aggregation group depends on hardware limitation.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Selected ports allowed in an aggregation group.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	1 to 4
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	1 to 4
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	1 to 4
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	1 to 4
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H	1 to 8

Hardware series	Model	Product code	Value range
		EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	1 to 8
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	1 to 8
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX20: 1 and 2 LSUM1WCMX20RT: 1 and 2 EWPXM2WCMD0F: 1 and 2 LSQM1WCMX40: 1 to 8 EWPXM1WCME0: 1 to 8 LSUM1WCME0: 1 to 8 LSUM1WCMX20RT: 1 and 2 LSUM1WCMX40RT: 1 to 8 EWPXM1MAC0F: 1 to 8

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	1 to 4
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	1 to 8
WX5800H series	WX5860H	EWP-WX5860H-GL	1 to 8

Usage guidelines

Executing this command might cause some of the Selected ports in an aggregation group to become Unselected ports.

The maximum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

The maximum number of Selected ports allowed in an aggregation group is limited by one of the following values, whichever value is smaller:

- Maximum number set by using the **`link-aggregation selected-port maximum`** command.
- Maximum number of Selected ports allowed by the link aggregation capability.

You can implement backup between two ports by performing the following tasks:

- Assigning two ports to an aggregation group.
- Setting the maximum number of Selected ports to 1 for the aggregation group.

Then, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port acts as a backup port.

Examples

Set the maximum number of Selected ports to 5 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

Related commands

link-aggregation selected-port minimum

link-aggregation selected-port minimum

Use **link-aggregation selected-port minimum** to set the minimum number of Selected ports in an aggregation group.

Use **undo link-aggregation selected-port minimum** to restore the default.

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

Default

The minimum number of Selected ports in an aggregation group is not specified.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

min-number: Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Fixed at 1
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2508H-PWR-LTE: Fixed at 1 WX2510H: Fixed at 1 WX2510H-F: Fixed at 1 WX2540H: Fixed at 1 WX2540H-F: Fixed at 1 WX2560H: 1 to 4
MAK series	MAK204	EWP-MAK204	1 to 4

Hardware series	Model	Product code	Value range
	MAK206	EWP-MAK206	
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Fixed at 1
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	1 to 8
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	1 to 8
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	1 to 8
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Fixed at 1

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Fixed at 1
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	1 to 8
WX5800H series	WX5860H	EWP-WX5860H-GL	1 to 8

Usage guidelines

Executing this command might cause all member ports in the aggregation group to become Unselected ports.

The minimum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

Examples

Set the minimum number of Selected ports to 3 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

Related commands

link-aggregation selected-port maximum

port link-aggregation group

Use **port link-aggregation group** to assign an interface to an aggregation group.

Use **undo port link-aggregation group** to remove an interface from the aggregation group to which it belongs.

Syntax

port link-aggregation group *group-id*

undo port link-aggregation group

Default

An interface does not belong to any aggregation group.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies an aggregation group by its aggregate interface number.

The following compatibility matrixes show the value ranges for this argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Fixed at 1
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Fixed at 1
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Fixed at 1
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H	1 to 2

Hardware series	Model	Product code	Value range
	WX3024H-L-PWR WX3024H-F	EWP-WX3024H-L-PWR EWP-WX3024H-F	
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: Fixed at 1 WX3510H: 1 to 4 WX3520H: 1 to 4 WX3520H-F: 1 to 4 WX3540H: 1 to 4
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 1 to 4 WX5540E: 1 to 6
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	1 to 6
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Fixed at 1

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Fixed at 1
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	1 to 4
WX5800H series	WX5860H	EWP-WX5860H-GL	1 to 6

Usage guidelines

You can assign a Layer 2 Ethernet interface only to a Layer 2 aggregation group.

An interface can belong to only one aggregation group.

Examples

Assign Layer 2 Ethernet interface GigabitEthernet 1/0/1 to Layer 2 aggregation group 1.

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

reset counters interface

Use **reset counters interface** to clear statistics for the specified aggregate interfaces.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you specify only an aggregate interface type, the command clears statistics for all aggregate interfaces of the specified type.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

Examples

Clear statistics for Layer 2 aggregate interface Bridge-Aggregation 1.

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

reset lacp statistics

Use **reset lacp statistics** to clear LACP statistics for the specified link aggregation member ports.

Syntax

reset lacp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number1* argument must be equal to or greater than the value for the *interface-number2* argument. If you do not specify any member ports, the command clears LACP statistics for all member ports.

Examples

Clear LACP statistics for all link aggregation member ports.

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

Related commands

display link-aggregation member-port

shutdown

Use **shutdown** to shut down an interface.

Use **undo shutdown** to bring up an interface.

Syntax

shutdown

undo shutdown

Default

An interface is not manually shut down.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Bring up Layer 2 aggregate interface Bridge-Aggregation 1.

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

Contents

Port isolation commands 1
display port-isolate group 2
port-isolate enable 3

Port isolation commands

The following compatibility matrixes show the support of hardware platforms for port isolation:

Hardware series	Model	Product code	Port isolation compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	No
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	No
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X-PWR • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	No

Hardware series	Model	Product code	Port isolation compatibility
	EWPXM2WCMD0F EWPXM1MAC0F	EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	Port isolation compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	No
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

display port-isolate group

Use **display port-isolate group** to display port isolation group information.

Syntax

display port-isolate group

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display port isolation group information.

```
<Sysname> display port-isolate group
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/2
```

Table 1 Command output

Field	Description
Group ID	ID of the isolation group.
Group members	Isolated ports in the isolation group. **No ports** indicates that the isolation group does not contain isolated ports.

Related commands

port-isolate enable

port-isolate enable

Use **port-isolate enable** to assign a port to an isolation group.

Use **undo port-isolate enable** to remove a port from an isolation group.

Syntax

port-isolate enable

undo port-isolate enable

Default

The port is not assigned to an isolation group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

The configuration in Layer 2 Ethernet interface view applies only to the interface.

The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the device fails to apply the configuration to the aggregate interface, it does not assign any aggregation member port to the isolation group. If the failure occurs on an aggregation member port, the device skips the port and continues to assign other aggregation member ports to the isolation group.

This command assigns a port to the default isolation group (isolation group 1).

Examples

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the default isolation group.

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

Assign Layer 2 aggregate interface **Bridge-Aggregation 1** to the default isolation group.

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

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

Related commands

display port-isolate group

Contents

DHCP commands 1

Common DHCP commands 1
dhcp client-detect 1
dhcp dscp 1
dhcp enable 2
dhcp log enable 2
dhcp select 3
DHCP server commands 4
address range 4
bims-server 5
bootfile-name 6
class ip-pool 7
class option-group 7
class range 8
default ip-pool 9
dhcp apply-policy 10
dhcp class 11
dhcp option-group 11
dhcp policy 12
dhcp server always-broadcast 13
dhcp server apply ip-pool 13
dhcp server bootp ignore 14
dhcp server bootp reply-rfc-1048 15
dhcp server database filename 15
dhcp server database update interval 17
dhcp server database update now 18
dhcp server database update stop 18
dhcp server forbidden-ip 19
dhcp server ip-pool 20
dhcp server ping packets 20
dhcp server ping timeout 21
dhcp server relay information enable 22
dhcp server reply-exclude-option60 22
display dhcp server conflict 23
display dhcp server database 24
display dhcp server expired 25
display dhcp server free-ip 25
display dhcp server ip-in-use 26
display dhcp server pool 28
display dhcp server statistics 30
dns-list 32
domain-name 32
expired 33
forbidden-ip 34
forbidden-ip-range 35
gateway-list 36
if-match 36
ip-in-use threshold 39
nbns-list 40
netbios-type 40
network 41
next-server 42
option 43
reset dhcp server conflict 44
reset dhcp server expired 45
reset dhcp server ip-in-use 45
reset dhcp server statistics 46

static-bind 46
tftp-server domain-name 47
tftp-server ip-address 48
valid class 49
verify class 49
DHCP relay agent commands 50
dhcp relay check mac-address 50
dhcp relay check mac-address aging-time 51
dhcp relay client-information record 51
dhcp relay client-information refresh 52
dhcp relay client-information refresh enable 53
dhcp relay forward reply by-option82 54
dhcp relay gateway 54
dhcp relay information circuit-id 55
dhcp relay information enable 57
dhcp relay information remote-id 57
dhcp relay information strategy 59
dhcp relay release ip 60
dhcp relay server-address 60
dhcp relay source-address 61
dhcp smart-relay enable 62
display dhcp relay check mac-address 63
display dhcp relay client-information 63
display dhcp relay information 64
display dhcp relay server-address 66
display dhcp relay statistics 66
gateway-list 68
remote-server 69
reset dhcp relay client-information 69
reset dhcp relay statistics 70
DHCP client commands 70
dhcp client dad enable 70
dhcp client dscp 71
dhcp client identifier 71
display dhcp client 72
ip address dhcp-alloc 75
DHCP snooping commands 75
dhcp snooping binding database filename 75
dhcp snooping binding database update interval 77
dhcp snooping binding database update now 78
dhcp snooping check mac-address 78
dhcp snooping deny 79
dhcp snooping enable 79
dhcp snooping information circuit-id 80
dhcp snooping information enable 82
dhcp snooping information remote-id 83
dhcp snooping information strategy 84
dhcp snooping log enable 85
dhcp snooping max-learning-num 86
dhcp snooping rate-limit 86
dhcp snooping trust 87
display dhcp snooping binding 88
display dhcp snooping binding database 89
display dhcp snooping information 90
display dhcp snooping packet statistics 91
display dhcp snooping trust 92
reset dhcp snooping binding 92
reset dhcp snooping packet statistics 93
BOOTP client commands 93
display bootp client 93
ip address bootp-alloc 94

DHCP commands

The MSG series, WX2500H-WiNet series, WAC series, WX2500H-LI series, and AC1000 series access controllers do not support parameters or commands that are available only in IRF mode.

Common DHCP commands

dhcp client-detect

Use **dhcp client-detect** to enable client offline detection on the DHCP server or DHCP relay agent.

Use **undo dhcp client-detect** to disable client offline detection on the DHCP server or DHCP relay agent.

Syntax

dhcp client-detect

undo dhcp client-detect

Default

Client offline detection is disabled on the DHCP server or DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The client offline detection feature on the DHCP server reclaims an assigned IP address and deletes the binding entry when the ARP entry ages out for the IP address.

This feature on the DHCP relay agent deletes the related relay entry and sends a RELEASE message to the DHCP server when an ARP entry ages out.

Examples

Enable client offline detection.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client-detect
```

dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server or the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP server or the DHCP relay agent.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP server or the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp dscp 30
```

dhcp enable

Use **dhcp enable** to enable DHCP.

Use **undo dhcp enable** to disable DHCP.

Syntax

dhcp enable

undo dhcp enable

Default

DHCP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP related configuration takes effect only after you enable DHCP.

Enable DHCP before you configure the DHCP server or relay agent.

Examples

Enable DHCP.

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

dhcp log enable

Use **dhcp log enable** to enable DHCP server logging.

Use **undo dhcp log enable** to disable DHCP server logging.

Syntax

dhcp log enable

undo dhcp log enable

Default

DHCP server logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP server to generate DHCP logs and send them to the information center. The information helps administrators to locate and solve problems. For information about the log destination and output rule configuration in the information center, see *System Management Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCP server logging.

```
<Sysname> system-view
[Sysname] dhcp log enable
```

dhcp select

Use **dhcp select** to enable the DHCP server or DHCP relay agent on an interface.

Use **undo dhcp select** to disable the DHCP server or DHCP relay agent on an interface. The interface will discard incoming DHCP packets.

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

Default

The interface operates in the DHCP server mode and responds to DHCP requests with configuration parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCP relay agent on the interface.

server: Enables the DHCP server on the interface.

Usage guidelines

Before enabling a DHCP server to operate as a DHCP relay agent, use the **reset dhcp server ip-in-use** command to clear address bindings and authorized ARP entries. These authorized ARP entries might conflict with ARP entries that are created after the DHCP relay agent is enabled.

When DHCP server proxy is enabled on the DHCP relay agent, the proxy forwards packets between the DHCP clients and DHCP server.

- When receiving DHCP requests from DHCP clients, the proxy forwards them to the DHCP server.
- When receiving DHCP responses from the DHCP server, the proxy modifies the DHCP server's IP address in these responses as its own IP address.

Examples

Enable the DHCP relay agent on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp select relay
```

Related commands

dhcp smart-relay enable

reset dhcp server ip-in-use

DHCP server commands

address range

Use **address range** to configure an IP address range in a DHCP address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ip-address end-ip-address*

undo address range

Default

No IP address range exists.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

If no IP address range is specified, all IP addresses in the subnet specified by the **network** command in address pool view are assignable. If an IP address range is specified, only the IP addresses in the IP address range are assignable.

After you use the **address range** command, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

If you execute this command multiple times, the most recent configuration takes effect.

The address range specified by the **address range** command must be within the subnet specified by the **network** command. The addresses outside of the subnet cannot be assigned.

Examples

Specify an address range of 192.168.8.1 through 192.168.8.150 in address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] network 192.168.8.1 mask 255.255.255.0
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

Related commands

class

dhcp class

display dhcp server pool

network

bims-server

Use **bims-server** to specify the IP address, port number, and shared key of the BIMS server in a DHCP address pool.

Use **undo bims-server** to restore the default.

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

Default

No BIMS server information is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters. The DHCP client uses the shared key to encrypt packets sent to the BIMS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify BIMS server IP address 1.1.1.1, port number 80, and shared key **aabbcc** in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

Related commands

display dhcp server pool

bootfile-name

Use **bootfile-name** to specify a configuration file name or URL.

Use **undo bootfile-name** to restore the default.

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

Default

No configuration file name or URL is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

bootfile-name: Specifies the configuration file name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

To specify a configuration file on a TFTP server, use the *bootfile-name* argument.

Examples

Specify configuration file name **boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg
```

Related commands

display dhcp server pool

next-server

tftp-server domain-name

tftp-server ip-address

class ip-pool

Use **class ip-pool** to specify a DHCP address pool for a DHCP user class.

Use **undo class ip-pool** to remove the DHCP address pool specified for a DHCP user class.

Syntax

class *class-name* **ip-pool** *pool-name*

undo class *class-name* **ip-pool**

Default

No DHCP address pool is specified for a DHCP user class.

Views

DHCP policy view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCP address pool for a DHCP user class in a DHCP policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** for DHCP user class **test** in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] class test ip-pool pool1
```

Related commands

default ip-pool

dhcp policy

dhcp server ip-pool

class option-group

Use **class option-group** to specify a DHCP option group for a DHCP user class.

Use **undo class option-group** to remove the configuration.

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

Default

No DHCP option group is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

option-group-number: Specifies a DHCP option group by its number in the range of 1 to 32768.

Usage guidelines

When receiving a DHCP-DISCOVER message, the server compares the client against the user classes in the order that they are specified by this command. If a match is found, the server assigns the client the DHCP options in the option group. If multiple matches are found, the server selects option groups by using the following methods:

- If the option groups have options in common, the server selects the option group specified for the first matching user class.
- If the option groups have different options, the server selects all the matching option groups.

You can specify only one option group for a DHCP user class in a DHCP address pool. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP option group 1 for user class **user** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] class user option-group 1
```

Related commands

dhcp option-group

class range

Use **class range** to specify an IP address range for a DHCP user class.

Use **undo class range** to remove the IP address range for the DHCP user class.

Syntax

class *class-name* **range** *start-ip-address end-ip-address*

undo class *class-name* **range**

Default

No IP address range is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class name, a case-insensitive string of 1 to 63 characters. If the specified user class does not exist, the DHCP server will not assign the addresses in the address range specified for the user class to any clients.

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

The **class range** command allows you to divide an address range into multiple address ranges for different DHCP user classes. The address range for a user class must be within the primary subnet specified by the **network** command. If the DHCP client does not match any DHCP user class, the DHCP server selects an address in the IP address range specified by the **address range** command. If the address range has no assignable IP addresses or no address range is configured, the address allocation fails.

After you specify an address range for a user class, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

You can specify only one address range for a DHCP user class in an address pool. If you execute this command multiple times for a DHCP user class, the most recent configuration takes effect.

Examples

Specify an IP address range of 192.168.8.1 through 192.168.8.150 for DHCP user class **user** in DHCP address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] class user range 192.168.8.1 192.168.8.150
```

Related commands

address range

dhcp class

display dhcp server pool

default ip-pool

Use **default ip-pool** to specify the default DHCP address pool.

Use **undo default ip-pool** to restore the default.

Syntax

default ip-pool *pool-name*

undo default ip-pool

Default

No default DHCP address pool is specified.

Views

DHCP policy view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCP policy, the DHCP server uses the default DHCP address pool to assign IP addresses and other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IP addresses, the address assignment fails.

You can specify only one default address pool in a DHCP policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** as the default DHCP address pool in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] default ip-pool pool1
```

Related commands

class ip-pool

dhcp policy

dhcp apply-policy

Use **dhcp apply-policy** to apply a DHCP policy to an interface.

Use **undo dhcp apply-policy** to restore the default.

Syntax

dhcp apply-policy *policy-name*

undo dhcp apply-policy

Default

No DHCP policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCP policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCP policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP policy **test** to VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp apply-policy test
```

Related commands

dhcp policy

dhcp class

Use **dhcp class** to create a DHCP user class and enter its view, or enter the view of an existing DHCP user class.

Use **undo dhcp class** to delete the specified DHCP user class.

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

Default

No DHCP user classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies the name of a DHCP user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCP user class view, you can use the **if-match** command to configure match rules to group clients to the user class.

Examples

Create DHCP user class **test** and enter DHCP user class view.

```
<Sysname> system-view
[Sysname] dhcp class test
[Sysname-dhcp-class-test]
```

Related commands

address range

class ip-pool

class option-group

class range

dhcp policy

if-match

dhcp option-group

Use **dhcp option-group** to create a DHCP option group and enter its view, or enter the view of an existing DHCP option group.

Use **undo dhcp option-group** to delete a DHCP option group.

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

Default

No DHCP option groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

option-group-number: Assigns a number to the DHCP option group, in the range of 1 to 32768.

Examples

Create DHCP option group 1 and enter DHCP option group view.

```
<Sysname> system-view
[Sysname] dhcp option-group 1
[Sysname-dhcp-option-group-1]
```

Related commands

class option-group

option

dhcp policy

Use **dhcp policy** to create a DHCP policy and enter its view, or enter the view of an existing DHCP policy.

Use **undo dhcp policy** to delete a DHCP policy.

Syntax

dhcp policy *policy-name*

undo dhcp policy *policy-name*

Default

No DHCP policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the DHCP policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IP addresses and other parameters from the specified address pool.

For a DHCP policy to take effect, you must apply it to an interface.

Examples

Create DHCP policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] dhcp policy test
[Sysname-dhcp-policy-test]
```

Related commands

`class ip-pool`

`default ip-pool`

`dhcp apply-policy`

`dhcp class`

dhcp server always-broadcast

Use **`dhcp server always-broadcast`** to enable the DHCP server to broadcast all responses.

Use **`undo dhcp server always-broadcast`** to restore the default.

Syntax

`dhcp server always-broadcast`

`undo dhcp server always-broadcast`

Default

The DHCP server reads the broadcast flag in a DHCP request to decide whether to broadcast or unicast the response.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP server to ignore the broadcast flag in DHCP requests and broadcast all responses.

The DHCP server always unicasts a response in the following situations, regardless of whether this command is executed:

- The DHCP request is from a DHCP client that has an IP address (the **ciaddr** field is not 0).
- The DHCP request is forwarded by a DHCP relay agent from a DHCP client (the **giaddr** field is not 0).

Examples

Enable the DHCP server to broadcast all responses.

```
<Sysname> system-view
[Sysname] dhcp server always-broadcast
```

dhcp server apply ip-pool

Use **`dhcp server apply ip-pool`** to apply an address pool to an interface.

Use **`undo dhcp server apply ip-pool`** to restore the default.

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

Default

No address pool is applied to an interface

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies the name of a DHCP address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Upon receiving a DHCP request from the interface, the DHCP server searches for a static binding for the client from all address pools. If no static binding is found, the server assigns configuration parameters from the address pool applied on the interface to the client. If the address pool has no assignable IP address or does not exist, the DHCP client cannot obtain an IP address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP address pool 0 to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp server apply ip-pool 0
```

Related commands

dhcp server ip-pool

dhcp server bootp ignore

Use **dhcp server bootp ignore** to configure the DHCP server to ignore BOOTP requests.

Use **undo dhcp server bootp ignore** to restore the default.

Syntax

dhcp server bootp ignore

undo dhcp server bootp ignore

Default

The DHCP server does not ignore BOOTP requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The lease duration of IP addresses obtained by BOOTP clients is unlimited. For scenarios that do not allow unlimited leases, you can configure the DHCP server to ignore BOOTP requests.

Examples

Configure the DHCP server to ignore BOOTP requests.

```
<Sysname> system-view
[Sysname] dhcp server bootp ignore
```

dhcp server bootp reply-rfc-1048

Use **dhcp server bootp reply-rfc-1048** to enable the sending of BOOTP responses in RFC 1048 format.

Use **undo dhcp server bootp reply-rfc-1048** to disable this feature.

Syntax

dhcp server bootp reply-rfc-1048

undo dhcp server bootp reply-rfc-1048

Default

This feature is disabled. The DHCP server does not process the Vend field of RFC 1048-incompliant requests but copies the Vend field into responses.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Not all BOOTP clients can send requests compliant with RFC 1048. This command enables the DHCP server to fill the Vend field in RFC 1048-compliant format in DHCP responses to RFC 1048-incompliant requests sent by BOOTP clients.

Examples

Enable the sending of BOOTP responses in RFC 1048 format on the DHCP server.

```
<Sysname> system-view
[Sysname] dhcp server bootp reply-rfc-1048
```

dhcp server database filename

Use **dhcp server database filename** to configure the DHCP server to back up the DHCP bindings to a file.

Use **undo dhcp server database filename** to restore the default.

Syntax

dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo dhcp server database filename

Default

The DHCP server does not back up the DHCP bindings.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file, a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCP server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **dhcp server database update interval** command to change the waiting time. If no DHCP binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCP server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.

If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.

- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCP server to back up its bindings to file **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp server database filename database.dhcp
```

Configure the DHCP server to back up its bindings to file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

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

```
[Sysname] dhcp server database filename url ftp://10.1.1.1/database.dhcp username 1
password simple 1
```

Related commands

dhcp server database update interval

dhcp server database update now

dhcp server database update stop

dhcp server database update interval

Use **dhcp server database update interval** to set the waiting time for the DHCP server to update the backup file after a DHCP binding change.

Use **undo dhcp server database update interval** to restore the default.

Syntax

dhcp server database update interval *interval*

undo dhcp server database update interval

Default

The DHCP server waits 300 seconds to update the backup file after a DHCP binding change. If no DHCP binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCP binding is created, updated, or removed, the waiting period starts. The DHCP server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCP binding auto backup by using the **dhcp server database filename** command.

Examples

Set the waiting time to 10 minutes for the DHCP server to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update interval 600
```

Related commands

dhcp server database filename

dhcp server database update now

dhcp server database update stop

dhcp server database update now

Use **dhcp server database update now** to manually save the DHCP bindings to the backup file.

Syntax

dhcp server database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCP bindings are saved to the backup file.

For this command to take effect, you must configure the DHCP auto backup by using the **dhcp server database filename** command.

Examples

Manually save the DHCP bindings to the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update now
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update stop

dhcp server database update stop

Use **dhcp server database update stop** to terminate the download of DHCP bindings from the backup file.

Syntax

dhcp server database update stop

Views

System view

Predefined user roles

network-admin

Usage guidelines

The DHCP server does not provide services during the binding download process. If the connection disconnects during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCP server stops waiting and starts providing address allocation services.

To enable the DHCP server to provide services without waiting for the connection to be repaired, use this command to terminate the download immediately. The IP addresses associated with the undownloaded bindings will be assigned to clients. Address conflicts might occur.

Examples

Terminate the download of the backup DHCP bindings.

```
<Sysname> system-view
[Sysname] dhcp server database update stop
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update now

dhcp server forbidden-ip

Use **dhcp server forbidden-ip** to exclude IP addresses from dynamic allocation globally.

Use **undo dhcp server forbidden-ip** to remove the configuration.

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

Default

No IP addresses are excluded from dynamic allocation globally.

Views

System view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address, which cannot be lower than the *start-ip-address*. If you do not specify this argument, only the *start-ip-address* is excluded from dynamic allocation.

Usage guidelines

The IP addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IP address is in a static DHCP binding, the address can still be assigned to the client.

The address or address range specified in the **undo dhcp server forbidden-ip** command must be the same as that specified in the **dhcp server forbidden-ip** command. To remove an IP address from the specified address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IP address ranges from dynamic allocation.

Examples

Exclude the IP addresses of 10.110.1.1 through 10.110.1.63 from dynamic allocation globally.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

Related commands

forbidden-ip

static-bind

dhcp server ip-pool

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view, or enter the view of an existing DHCP address pool.

Use **undo dhcp server ip-pool** to delete the specified DHCP address pool.

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Default

No DHCP address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCP address pool name, a case-insensitive string of 1 to 63 characters. The pool name uniquely identifies an address pool.

Usage guidelines

A DHCP address pool is used to store the configuration parameters to be assigned to DHCP clients.

Examples

Create a DHCP address pool named **pool1**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

Related commands

class ip-pool

dhcp server apply ip-pool

display dhcp server pool

dhcp server ping packets

Use **dhcp server ping packets** to set the maximum number of ping packets.

Use **undo dhcp server ping packets** to restore the default.

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

Default

The maximum number of ping packets is 1.

Views

System view

Predefined user roles

network-admin

Parameters

number: Sets the maximum number of ping packets, in the range of 0 to 10. To disable the address conflict detection, set the value to 0.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the maximum number of ping packets to 10.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

Related commands

dhcp server ping timeout

display dhcp server conflict

reset dhcp server conflict

dhcp server ping timeout

Use **dhcp server ping timeout** to set the ping response timeout time on the DHCP server.

Use **undo dhcp server ping timeout** to restore the default.

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

Default

The ping response timeout time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the timeout time in the range of 0 to 10000 milliseconds. To disable the ping operation for address conflict detection, set the value to 0 milliseconds.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the response timeout time to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

Related commands

dhcp server ping packets

display dhcp server conflict

reset dhcp server conflict

dhcp server relay information enable

Use **dhcp server relay information enable** to enable the DHCP server to handle Option 82.

Use **undo dhcp server relay information enable** to configure the DHCP server to ignore Option 82.

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

Default

The DHCP server handles Option 82.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Upon receiving a DHCP request that contains Option 82, the server copies the original Option 82 into the response. If the server is configured to ignore Option 82, the response will not contain Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

dhcp server reply-exclude-option60

Use **dhcp server reply-exclude-option60** to disable the DHCP server from encapsulating Option 60 in DHCP replies.

Use **undo dhcp server reply-exclude-option60** to restore the default.

Syntax

dhcp server reply-exclude-option60

undo dhcp server reply-exclude-option60

Default

The DHCP server can encapsulate Option 60 in DHCP replies.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you do not disable the capability, the DHCP server encapsulates Option 60 in a DHCP reply in the following situations:

- The received DHCP packet contains Option 60.
- Option 60 is configured for the address pool.

If you disable the capability, the DHCP server does not encapsulate Option 60 in DHCP replies.

Examples

Disable the DHCP server from encapsulating Option 60 in DHCP replies.

```
<Sysname> system-view
[Sysname] dhcp server reply-exclude-option60
```

display dhcp server conflict

Use **display dhcp server conflict** to display information about IP address conflicts.

Syntax

display dhcp server conflict [**ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays conflict information about the specified IP address. If you do not specify this option, this command displays information about all IP address conflicts.

Usage guidelines

The DHCP server generates IP address conflict information in the following situations:

- Before assigning an IP address to a DHCP client, the DHCP server pings the IP address and discovers that another host is using the address.
- The DHCP client sends a DECLINE packet to the DHCP server to inform the server of an IP address conflict.
- The DHCP server discovers that the only assignable address in the address pool is its own IP address.

Examples

Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict
IP address          Detect time
4.4.4.1             Apr 25 16:57:20 2019
4.4.4.2             Apr 25 17:00:10 2019
```

Table 1 Command output

Field	Description
IP address	Conflicted IP address.
Detect time	Time when the conflict was discovered.

Related commands

`reset dhcp server conflict`

display dhcp server database

Use **`display dhcp server database`** to display information about DHCP binding auto backup.

Syntax

`display dhcp server database`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCP binding auto backup.

```
<Sysname> display dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
 Latest write time       :   Feb  8 16:09:53 2014
 Status                  :   Last write succeeded.
```

Table 2 Command output

Field	Description
File name	Name of the DHCP binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCP binding change for the DHCP server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp server expired

Use **display dhcp server expired** to display the lease expiration information.

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays lease expiration information about the specified IP address. If you do not specify an IP address, this command displays lease expiration information about all IP addresses.

pool *pool-name*: Displays lease expiration information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays lease expiration information about all address pools.

Usage guidelines

DHCP assigns these expired IP addresses to DHCP clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display dhcp server expired
IP address       Client-identifier/Hardware address    Lease expiration
4.4.4.6          3030-3066-2e65-3230-302e-3130-3234    Apr 25 17:10:47 2019
                 -2d45-7468-6572-6e65-7430-2f31
```

Table 3 Command output

Field	Description
IP address	Expired IP address.
Client-identifier/Hardware address	Client ID or MAC address. For the client ID: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of an interface is used as the client ID value, the type value is 01. • If a hexadecimal string is used as the client ID value, the type value is the first two digits of the string.
Lease expiration	Time when the lease expired.

Related commands

reset dhcp server expired

display dhcp server free-ip

Use **display dhcp server free-ip** to display information about assignable IP addresses.

Syntax

display dhcp server free-ip [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays assignable IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays all assignable IP addresses for all address pools.

Examples

Display assignable IP addresses in all address pools.

```
<Sysname> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.1 to 10.0.0.254
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.1 to 10.1.0.254

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.1 to 20.1.1.254
```

Table 4 Command output

Field	Description
Pool name	Name of the address pool.
Network	Assignable network.
IP ranges	Assignable IP address range.
Secondary networks	Assignable secondary networks.

Related commands

address range

dhcp server ip-pool

network

display dhcp server ip-in-use

Use **display dhcp server ip-in-use** to display binding information about assigned IP addresses.

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays binding information about the specified assigned IP address. If you do not specify an IP address, this command displays binding information about all assigned IP addresses.

pool *pool-name*: Displays binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays binding information about assigned IP addresses in all address pools.

Usage guidelines

The binding information can be used by other security modules only when the DHCP server is configured on the gateway of DHCP clients.

If the lease deadline exceeds the year 2100, the lease expiration time is displayed as **After 2100**.

Examples

Display binding information about all assigned DHCP addresses.

```
<Sysname> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.1         4444-4444-4444        Not used              Static(F)
10.1.1.2         0030-3030-302e-3030-  May 1 14:02:49 2015   Auto(C)
                 3066-2e30-3030-332d-
                 4574-6865-726e-6574
10.1.1.3         1111-1111-1111        After 2100            Static(C)
```

Table 5 Command output

Field	Description
IP address	IP address assigned.
Client identifier/Hardware address	Client ID or hardware address. Client ID is specified as a string of hexadecimal numbers, in which the first two characters represents the hardware type value. • If an ASCII string is used, the hardware type value is 00, which means no type. • If the hardware type is Ethernet, the type value is 01. • If the hardware type is token ring, the type value is 06.
Lease expiration	Lease expiration time: • **Exact time (May 1 14:02:49 2015 in this example)**—Time when the lease will expire. • **Not used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time. • **After 2100**—The lease will expire after 2100.
Type	Binding types: • **Static(F)**—A free static binding whose IP address has not been

Field	Description
	assigned. • **Static(O)**—An offered static binding whose IP address has been selected and sent by the DHCP server in a DHCP-OFFER packet to the client. **Static(C)**—A committed static binding whose IP address has been assigned to the DHCP client. • **Auto(O)**—An offered dynamic binding whose IP address has been dynamically selected by the DHCP server and sent in a DHCP-OFFER packet to the DHCP client. • **Auto(C)**—A committed dynamic binding whose IP address has been dynamically assigned to the DHCP client.

Related commands

reset dhcp server ip-in-use

display dhcp server pool

Use **display dhcp server pool** to display information about a DHCP address pool.

Syntax

display dhcp server pool [*pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify the *pool-name* argument, this command displays information about all address pools.

Examples

Display information about all DHCP address pools.

```
<Sysname> display dhcp server pool
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.2.0 mask 255.255.255.0
  secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
```

```
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
  nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.3.0 mask 255.255.255.0
  address range 20.1.3.1 to 20.1.3.15
  class departmentA range 20.1.3.20 to 20.1.3.29
  class departmentB range 20.1.3.30 to 20.1.3.40
  next-server 20.1.3.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 20.1.3.2
  voice-config as-ip 20.1.3.5
  voice-config fail-over 20.1.3.6 123*
  option 2 ip-address 20.1.3.10
  expired 1 0 0 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

Table 6 Command output

Field	Description
Pool name	Name of an address pool.
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class *class-name* range	DHCP user class and its address range.
static bindings	Static IP-to-MAC/client ID bindings.
option	Customized DHCP option.
expired	Lease duration: 1 2 3 4 in this example refers to 1 day 2 hours 3 minutes 4 seconds.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.

Field	Description
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config fail-over	Failover route.

display dhcp server statistics

Use **display dhcp server statistics** to display the DHCP server statistics.

Syntax

display dhcp server statistics [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Specifies an address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, this command displays information about all address pools.

Examples

Display the DHCP server statistics.

```
<Sysname> display dhcp server statistics
    Pool number:                      1
    Pool utilization:                 0.39%
    Bindings:
      Automatic:                      1
      Manual:                         0
      Expired:                        0
    Conflict:                         1
    Messages received:               10
      DHCPDISCOVER:                   5
      DHCPREQUEST:                    3
```

```
    DHCPDECLINE:                0
    DHCPRELEASE:                2
    DHCPINFORM:                 0
    BOOTPREQUEST:               0
  Messages sent:                6
    DHCPOFFER:                  3
    DHCPACK:                    3
    DHCPNAK:                    0
    BOOTPREPLY:                 0
  Bad Messages:                 0
```

Table 7 Command output

Field	Description
Pool number	Total number of address pools. This field is not displayed when you display statistics for a specific address pool.
Pool utilization	Pool usage rate: • If you display statistics for all address pools, this field displays the usage rate of all address pools. • If you display statistics for an address pool, this field displays the pool usage rate of the specified address pool.
Bindings	Bindings include the following types: • **Automatic**—Number of dynamic bindings. • **Manual**—Number of static bindings. • **Expired**—Number of expired bindings.
Conflict	Total number of conflict addresses. This field is not displayed if you display statistics for a specific address pool.
Messages received	DHCP packets received from clients: • DHCPDISCOVER. • DHCPREQUEST. • DHCPDECLINE. • DHCPRELEASE. • DHCPINFORM. • BOOTPREQUEST. This field is not displayed if you display statistics for a specific address pool.
Messages sent	DHCP packets sent to clients: • DHCPOFFER. • DHCPACK. • DHCPNAK. • BOOTPREPLY. This field is not displayed if statistics about a specific address pool are displayed.
Bad Messages	Number of bad messages. This field is not displayed if you display statistics for a specific address pool.

Related commands

reset dhcp server statistics

dns-list

Use **dns-list** to specify DNS server addresses in a DHCP address pool.

Use **undo dns-list** to remove DNS server addresses from a DHCP address pool.

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

Default

No DNS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DNS servers.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo dns-list** command deletes all DNS server addresses in the DHCP address pool.

Examples

Specify DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

Related commands

display dhcp server pool

domain-name

Use **domain-name** to specify a domain name in a DHCP address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify domain name **company.com** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com
```

Related commands

display dhcp server pool

expired

Use **expired** to set the lease duration in a DHCP address pool.

Use **undo expired** to restore the default lease duration for a DHCP address pool.

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

Default

The lease duration of a dynamic DHCP address pool is one day.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23. The default is 0.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59. The default is 0.

second *second*: Specifies the number of seconds, in the range of 0 to 59. The default is 0.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Usage guidelines

The DHCP server assigns an IP address together with the lease duration to the DHCP client. Before the lease expires, the DHCP client must extend the lease duration.

- If the lease extension operation succeeds, the DHCP client can continue to use the IP address.
- If the lease extension operation does not succeed, both of the following events occur:
  - The DHCP client cannot use the IP address after the lease duration expires.
  - The DHCP server will label the IP address as an expired address.

Examples

Set the lease duration to 1 day, 2 hours, 3 minutes, and 4 seconds 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 second 4
```

Related commands

display dhcp server expired

display dhcp server pool

reset dhcp server expired

forbidden-ip

Use **forbidden-ip** to exclude IP addresses from dynamic allocation in an address pool.

Use **undo forbidden-ip** to remove the configuration.

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

Default

No IP addresses are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight excluded IP addresses.

Usage guidelines

The excluded IP addresses in an address pool are still assignable in other address pools.

You can exclude a maximum of 4096 IP addresses in an address pool by executing this command multiple times.

If you do not specify any parameters, the **undo forbidden-ip** command removes all excluded IP addresses.

Examples

Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

Related commands

dhcp server forbidden-ip

display dhcp server pool

forbidden-ip-range

Use **forbidden-ip-range** to exclude an IP address range from DHCP allocation in an address pool.

Use **undo forbidden-ip-range** to remove an IP address range from the forbidden IP range list.

Syntax

forbidden-ip-range *start-ip-address* [*end-ip-address*]

undo forbidden-ip-range [*start-ip-address* [*end-ip-address*]]

Default

No IP address ranges are excluded from DHCP allocation in an address pool.

Views

IP address pool view

Predefined user roles

network-admin

mdc-admin

Parameters

start-ip-address: Specifies a start IP address.

end-ip-address: Specifies an end IP address. The end IP address cannot be lower than the start IP address. If you do not specify this argument, the excluded IP range includes only the start IP address.

Usage guidelines

The forbidden IP ranges in an address pool are still assignable in other address pools.

To specify multiple forbidden IP ranges, execute the **forbidden-ip-range** command multiple times. The forbidden IP ranges can overlap.

When you execute the **undo** form of this command to remove forbidden IP ranges, follow these guidelines:

- To remove all forbidden IP ranges, execute the **undo forbidden-ip-range** command without specifying any parameters.
- To remove a subrange of IP addresses from a forbidden IP range, specify only that subrange of IP addresses.
- To remove a forbidden IP range as a whole, specify that IP range or an IP range broader than it.

Examples

Exclude IP address range 192.168.1.3 to 192.168.1.10 from DHCP allocation in IP address pool **0**.

```
<Sysname> system-view
[Sysname] ip pool pool0
[Sysname-ip-pool-pool0] forbidden-ip-range 192.168.1.3 192.168.1.10
```

Related commands

display dhcp server pool

gateway-list

Use **gateway-list** to specify gateway addresses in a DHCP address pool or a DHCP secondary subnet.

Use **undo gateway-list** to remove the specified gateway addresses from a DHCP address pool or a DHCP secondary subnet.

Syntax

gateway-list *ip-address*&<1-64> [**export-route**]

undo gateway-list [*ip-address*&<1-64>] [**export-route**]

Default

No gateway address is configured in a DHCP address pool or a DHCP secondary subnet.

Views

DHCP address pool view

DHCP secondary subnet view

Predefined user roles

network-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 gateway addresses. Gateway addresses must reside on the same subnet as the assignable IP addresses.

export-route: Binds the gateways to the device's MAC address in the address management module. The ARP module will use the entries to reply to ARP requests from the DHCP clients. If you do not specify this keyword, the gateways will not be bound to the device's MAC address.

Usage guidelines

The DHCP server assigns gateway addresses to clients on a secondary subnet in the following ways:

- If gateways are specified in both address pool view and secondary subnet view, DHCP assigns those specified in the secondary subnet view.
- If gateways are specified in address pool view but not in secondary subnet view, DHCP assigns those specified in address pool view.

If you do not specify any parameters, the **undo gateway-list** command deletes all gateway addresses.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

display dhcp server pool

if-match

Use **if-match** to configure a match rule for a DHCP user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **hardware-address** *hardware-address* **mask** *hardware-address-mask* | **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCP user class.

Views

DHCP user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 128. A smaller ID represents a higher match priority.

hardware-address *hardware-address*: Specifies a hardware address, a string of 4 to 39 characters. The string contains hyphen-separated hexadecimal numbers. The last hexadecimal number can be a two-digit or four-digit number, and the other hexadecimal numbers must be four-digit numbers. For example, **aabb-ccdd-ee** is valid, and **aabb-c-dddd** or **aabb-cc-dddd** is invalid.

mask *hardware-address-mask*: Specifies the mask to be ANDed with the specified hardware address for the match operation. The length of the mask must be the same as that of the hardware address.

option *option-code*: Specifies a DHCP option by its number in the range of 1 to 254.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 254. If you do not specify an offset value, the match starts from the first byte of the option content. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches a rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies a hexadecimal mask for the match operation. The mask length must be an even number in the range of 2 to 256 and be the same as the *hex-string* length. The DHCP server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-address*: Specifies a **giaddr** field value. The value is an IPv4 address in the dotted decimal notation. A packet matches the rule if its **giaddr** field value is the same as that in the rule.

Usage guidelines

If a DHCP request sent by a DHCP client matches a rule in a DHCP user class, the DHCP client matches the user class.

You can configure multiple match rules for a DHCP user class. Each match rule is uniquely identified by a rule ID within its type (hardware address, option, or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.
- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.
- Rules of different IDs cannot have the same rule content.

When you configure an **if-match hardware-address** rule, follow these guidelines:

- The hardware address type supports only the MAC address. A rule does not match clients with hardware addresses of other types.
- The specified hardware address must be of the same length as the client hardware addresses to be matched. To match MAC addresses, the specified hardware address must be six bytes long.
- The fs and 0s in the mask for the hardware match operation can be noncontiguous. For example, the rule **if-match rule** 1 **hardware-address** 0094-0000-1100 **mask** ffff-0000-ff00 matches hardware addresses in which the first two bytes are 0094 and the fifth byte is 11.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for DHCP user class **exam** to match DHCP requests in which the hardware address is six bytes long and begins with **0094**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 1 hardware-address 0094-0000-0101 mask
ffff-0000-0000
```

Configure match rule **2** for DHCP user class **exam** to match DHCP requests that contain Option 82.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82
```

Configure match rule **3** for DHCP user class **exam**. The rule matches DHCP requests in which the highest bit of the fourth byte in Option 82 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] dhcp class exam
```

```
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

Configure match rule **4** for DHCP user class **exam**. The rule matches DHCP requests in which the first three bytes of Option 82 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 4 option 82 hex 13ae92 offset 0 length 3
```

Configure match rule **5** for DHCP user class **exam**. The rule matches DHCP requests in which the Option 82 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 5 option 82 hex 13ae partial
```

Configure match rule **6** for DHCP user class **exam** to match DHCP requests in which the **giaddr** field is 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 6 relay-agent 10.1.1.1
```

Related commands

dhcp class

ip-in-use threshold

Use **ip-in-use threshold** to set a threshold for the address pool usage alarming.

Use **undo ip-in-use threshold** to restore the default.

Syntax

ip-in-use threshold *threshold-value*

undo ip-in-use threshold

Default

The address pool usage threshold is 100%.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold for the address pool usage percentage. The value range is 1 to 100.

Usage guidelines

If you execute this command in the same address pool view multiple times, the most recent configuration takes effect.

When the address pool usage exceeds the threshold, the system sends log messages to the information center. According to the log information, you can optimize the address pool configuration. For more information about the information center, see *System Management Configuration Guide*.

Examples

Set the address pool usage threshold to 85%.

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

```
[Sysname] dhcp server ip-pool p1
[Sysname-dhcp-pool-p1] ip-in-use threshold 85
```

nbns-list

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

Default

No WINS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight WINS server IP addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo nbns-list** command deletes all WINS server addresses.

Examples

Specify WINS server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1
```

Related commands

display dhcp server pool

netbios-type

netbios-type

Use **netbios-type** to specify the NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to restore the default.

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Default

No NetBIOS node type is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

b-node: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server. If it does not receive a response, the h-node client broadcasts the destination name to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name. If it does not receive a response, the m-node client unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the NetBIOS node type as p-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type p-node
```

Related commands

display dhcp server pool

nbns-list

network

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**export-route**] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

Default

No subnet is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length or mask is specified, the natural mask will be used.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask in dotted decimal format.

export-route: Advertises the subnet assigned to DHCP clients. If you do not specify this keyword, the subnet will not be advertised.

secondary: Specifies the subnet as a secondary subnet. If you do not specify this keyword, this command specifies the primary subnet. If the addresses in the primary subnet are used up, the DHCP server can select addresses from a secondary subnet for clients.

Usage guidelines

You can use the **secondary** keyword to specify a secondary subnet and enter its view. In secondary subnet view, you can specify gateways by using the **gateway-list** command for DHCP clients in the secondary subnet.

You can specify only one primary subnet for a DHCP address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

You can specify up to 32 secondary subnets for a DHCP address pool.

The primary subnet and secondary subnets in a DHCP address pool must not have the same network address and mask.

If you have used the **address range** or **class** command in an address pool, you cannot specify a secondary subnet in the same address pool.

Modifying or removing the **network** configuration deletes the assigned addresses from the current address pool.

If you execute the **network export-route** command multiple times, the most recent configuration takes effect.

Examples

Specify primary subnet 192.168.8.0/24 and secondary subnet 192.168.10.0/24 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
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]
```

Related commands

display dhcp server pool

gateway-list

next-server

Use **next-server** to specify the IP address of a server in a DHCP address pool.

Use **undo next-server** to restore the default.

Syntax

next-server *ip-address*

undo next-server

Default

No server's IP address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a server.

Usage guidelines

Upon startup, the DHCP client obtains an IP address and the specified server IP address. Then it contacts the specified server, such as a TFTP server, to get other boot information.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify a server's IP address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254
```

Related commands

display dhcp server pool

option

Use **option** to customize a DHCP option.

Use **undo option** to remove a customized DHCP option.

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

Default

No DHCP option is customized.

Views

DHCP address pool view

DHCP option group view

Predefined user roles

network-admin

Parameters

code: Specifies the number of the customized option, in the range of 2 to 254, excluding 50 through 54, 56, 58, 59, 61, and 82.

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 255 characters as the option content.

hex *hex-string*: Specifies a hexadecimal number as the option content. The length of the hexadecimal number must be an even number in the range of 2 to 256.

ip-address *ip-address*&<1-8>: Specifies a space-separated list of up to eight IP addresses as the option content.

Usage guidelines

The DHCP server fills the customized option with the specified ASCII string, hexadecimal number, or IP addresses, and sends it in a response to the client.

You can customize options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command. For example, you can use the **option 4 ip-address 1.1.1.1** command to define the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration command. For example, the **dns-list** command can specify up to eight DNS servers. To specify more than eight DNS server, you must use the **option 6** command to define all DNS servers.

DHCP options specified by dedicated commands take precedence over those specified by the **option** commands. For example, if a DNS server address is specified by both the **dns-list** command and the **option 6** command, the server uses the address specified by the **dns-list** command.

DHCP options specified in DHCP option groups take precedence over those specified in DHCP address pools.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 7 to specify log server address 2.2.2.2 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

Related commands

display dhcp server pool

reset dhcp server conflict

Use **reset dhcp server conflict** to clear IP address conflict information.

Syntax

reset dhcp server conflict [**ip** *ip-address*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears conflict information about the specified IP address. If you do not specify this option, this command clears all address conflict information.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After you modify the address pool configuration, the conflicted addresses might become assignable. To assign these addresses, use the **reset dhcp server conflict** command to clear the conflict information first.

Examples

Clear all IP address conflict information.

```
<Sysname> reset dhcp server conflict
```

Related commands

display dhcp server conflict

reset dhcp server expired

Use **reset dhcp server expired** to clear binding information about expired IP addresses.

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified expired IP address. If you do not specify an IP address, this command clears binding information about all expired IP addresses.

pool *pool-name*: Clears binding information about the expired IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about expired IP addresses in all address pools.

Examples

Clear binding information about all expired IP addresses.

```
<Sysname> reset dhcp server expired
```

Related commands

display dhcp server expired

reset dhcp server ip-in-use

Use **reset dhcp server ip-in-use** to clear binding information about assigned IP addresses.

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified assigned IP address. If you do not specify an IP address, this command clears binding information about all assigned IP addresses.

pool *pool-name*: Clears binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about assigned IP addresses in all address pools.

Usage guidelines

If you use this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information about IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

Related commands

display dhcp server ip-in-use

reset dhcp server statistics

Use **reset dhcp server statistics** to clear DHCP server statistics.

Syntax

reset dhcp server statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear DHCP server statistics.

```
<Sysname> reset dhcp server statistics
```

Related commands

display dhcp server statistics

static-bind

Use **static-bind** to statically bind a client ID or MAC address to an IP address.

Use **undo static-bind** to remove a static binding.

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

undo static-bind ip-address *ip-address*

Default

No static binding is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address *ip-address*: Specifies the IP address of the static binding. The natural mask is used if no mask length or mask is specified.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask, in dotted decimal format.

client-identifier *client-identifier*: Specifies the client ID of the static binding, a string of 4 to 254 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

hardware-address *hardware-address*: Specifies the client hardware address of the static binding, a string of 4 to 39 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

ethernet: Specifies the client hardware address type as Ethernet. The default type is Ethernet.

token-ring: Specifies the client hardware address type as token ring.

Usage guidelines

The IP address of a static binding must not be an interface address of the DHCP server. Otherwise, an IP address conflict occurs, and the bound client cannot obtain the IP address.

You can specify multiple static bindings in an address pool. The total number of static bindings in all address pools cannot exceed 8192.

An IP address can be bound to only one DHCP client. To modify the binding for a DHCP client, first execute the **undo** form of the command to delete the existing binding and then create a new binding.

Examples

Bind IP address 10.1.1.1/24 to client ID **00aa-aabb** 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
client-identifier 00aa-aabb
```

Related commands

display dhcp server pool

tftp-server domain-name

Use **tftp-server domain-name** to specify a TFTP server name in a DHCP address pool.

Use **undo tftp-server domain-name** to restore the default.

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

Default

No TFTP server name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the TFTP server name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server name **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

Related commands

display dhcp server pool

tftp-server ip-address

tftp-server ip-address

Use **tftp-server ip-address** to specify a TFTP server address in a DHCP address pool.

Use **undo tftp-server ip-address** to restore the default.

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

Default

No TFTP server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a TFTP server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 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
```

Related commands

display dhcp server pool

tftp-server domain-name

valid class

Use **valid class** to add DHCP user classes to the whitelist.

Use **undo valid class** to remove DHCP user classes from the whitelist.

Syntax

valid class *class-name*&<1-8>

undo valid class *class-name*&<1-8>

Default

No DHCP user class is listed on the whitelist.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name&<1-8>: Specifies a space-separated list of up to eight DHCP user classes by their names, a case-insensitive string of 1 to 63 characters.

Usage guidelines

For this command to take effect, you must enable the DHCP user class whitelist.

Examples

Add DHCP user classes **test1** and **test2** to the whitelist in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] valid class test1 test2
```

Related commands

dhcp class

verify class

verify class

Use **verify class** to enable the DHCP user class whitelist.

Use **undo verify class** to disable the DHCP user class whitelist.

Syntax

verify class

undo verify class

Default

The DHCP user class whitelist is disabled.

Views

DHCP address pool view

Predefined user roles

network-admin

Usage guidelines

After you enable the DHCP user class whitelist, the DHCP server processes requests only from clients on the DHCP user class whitelist.

The DHCP user class whitelist does not take effect on clients that request static IP addresses, and the server always processes their requests.

Examples

Enable the DHCP user class whitelist in DHCP address pool 0.

```
[Sysname] system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] verify class
```

Related commands

valid class

DHCP relay agent commands

dhcp relay check mac-address

Use **dhcp relay check mac-address** to enable MAC address check on the relay agent.

Use **undo dhcp relay check mac-address** to disable MAC address check on the relay agent.

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

Default

The MAC address check feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This feature enables the DHCP relay agent to compare the **chaddr** field of a received DHCP request with the source MAC address in the frame header. If they are the same, the DHCP relay agent forwards the request to the DHCP server. If they are not the same, the DHCP relay agent discards the request.

The MAC address check feature takes effect only when the **dhcp select relay** command has already been configured on the interface.

Enable the MAC address check feature only on the DHCP relay agent directly connected to the DHCP clients. A DHCP relay agent changes the source MAC address of DHCP packets before sending them.

Examples

Enable MAC address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay check mac-address
```

Related commands

dhcp select relay

dhcp relay check mac-address aging-time

Use **dhcp relay check mac-address aging-time** to set the aging time for MAC address check entries on the DHCP relay agent.

Use **undo dhcp relay check mac-address aging-time** to restore the default.

Syntax

dhcp relay check mac-address aging-time *time*

undo dhcp relay check mac-address aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the aging time for MAC address check entries, in the range of 30 to 600 seconds.

Usage guidelines

This command takes effect only after you execute the **dhcp relay check mac-address** command.

Examples

Set the aging time to 60 seconds for MAC address check entries on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay check mac-address aging-time 60
```

dhcp relay client-information record

Use **dhcp relay client-information record** to enable recording client information in relay entries.

Use **undo dhcp relay client-information record** to disable the feature.

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

Default

The DHCP relay agent does not record client information in relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Client information is recorded only when the DHCP relay agent is configured on the gateway of DHCP clients. A relay entry contains information about a client such as the client's IP and MAC addresses.

Disabling the recording of client information deletes all recorded relay entries.

Examples

Enable the recording of relay entries on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay client-information record
```

Related commands

dhcp relay client-information refresh

dhcp relay client-information refresh enable

dhcp relay client-information refresh

Use **dhcp relay client-information refresh** to set the interval at which the DHCP relay agent refreshes relay entries.

Use **undo dhcp relay client-information refresh** to restore the default.

Syntax

dhcp relay client-information refresh [**auto** | **interval** *interval*]

undo dhcp relay client-information refresh

Default

The refresh interval is automatically calculated based on the number of relay entries.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Automatically calculates the refresh interval. The more the entries, the shorter the refresh interval. The shortest interval is 50 ms.

interval *interval*: Specifies the refresh interval in the range of 1 to 120 seconds.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay client-information refresh interval 100
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh enable

dhcp relay client-information refresh enable

Use **dhcp relay client-information refresh enable** to enable the DHCP relay agent to periodically refresh dynamic relay entries.

Use **undo dhcp relay client-information refresh enable** to disable the DHCP relay agent to periodically refresh dynamic relay entries.

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

Default

The DHCP relay agent periodically refreshes relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses a client's IP address and the relay interface's MAC address to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent performs the following operations:
  - Removes the relay entry.
  - Sends a DHCP-RELEASE message to the DHCP server to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the entry.

With this feature disabled, the DHCP relay agent does not remove relay entries automatically. After a DHCP client releases its IP address, you must use the **reset dhcp relay client-information** on the relay agent to remove the corresponding relay entry.

Examples

Disable periodic refresh of relay entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh

reset dhcp relay client-information

dhcp relay forward reply by-option82

Use **dhcp relay forward reply by-option82** to configure the DHCP relay agent to forward DHCP replies based on Option 82.

Use **undo dhcp relay forward reply by-option82** to restore the default.

Syntax

dhcp relay forward reply by-option82

undo dhcp relay forward reply by-option82

Default

The DHCP relay agent does not forward DHCP replies based on Option 82.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only after you execute the **dhcp relay information enable** and **dhcp relay information circuit-id** commands.

Examples

Configure the DHCP relay agent to forward DHCP replies based on Option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay forward reply by-option82
```

Related commands

dhcp relay information circuit-id

dhcp relay information enable

dhcp relay gateway

Use **dhcp relay gateway** to specify the DHCP relay agent address to be inserted in DHCP requests.

Use **undo dhcp relay gateway** to restore the default.

Syntax

dhcp relay gateway *ip-address*

undo dhcp relay gateway

Default

The primary IP address of the interface is inserted in DHCP requests as the DHCP relay agent address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the DHCP relay agent address. It must be an IP address of the interface.

Usage guidelines

The DHCP relay agent uses the specified IP address instead of the primary IP address of the relay interface as the DHCP relay agent address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10.1.1.1 as the DHCP relay agent address to be inserted in DHCP requests on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay gateway 10.1.1.1
```

Related commands

gateway-list

dhcp relay information circuit-id

Use **dhcp relay information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option of Option 82.

Use **undo dhcp relay information circuit-id** to restore the default.

Syntax

dhcp relay information circuit-id { **bas** | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

bas: Specifies the bas mode that fills in the Circuit ID sub-option with the interface and VLAN information. The device fills the informaton in the format of *interface-type slot/subslot/port vxlan_id.vlan_id.subvlan_id*.

string *circuit-id*: Specifies the string mode that uses a case-sensitive string of 3 to 63 characters as the content of the Circuit ID sub-option.

normal: Specifies the normal mode, in which the padding content consists of the VLAN ID and port number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format. If you specify this keyword, do not include any spaces when you set the device name. Otherwise, the DHCP relay agent fails to add or replace Option 82.
- **user-defined** *node-identifier:* Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

interface: Uses the interface name as the interface information. The padding format for the interface name is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 8 shows how the padding format is determined for different modes.

Table 8 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Specify the content mode as verbose, node identifier as the device name, and the padding format as ASCII for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier
sysname format ascii
```

Related commands

dhcp relay forward reply by-option82

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information enable

Use **dhcp relay information enable** to enable the DHCP relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

Syntax

dhcp relay information enable

undo dhcp relay information enable

Default

The DHCP relay agent does not support Option 82.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP relay agent to add Option 82 to DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp relay information circuit-id** and **dhcp relay information remote-id** commands. If the DHCP requests contain Option 82, the relay agent handles the requests according to the strategy configured with the **dhcp relay information strategy** command.

If this feature is disabled, the relay agent forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
```

Related commands

dhcp relay forward reply by-option82

dhcp relay information circuit-id

dhcp relay information remote-id

dhcp relay information strategy

display dhcp relay information

dhcp relay information remote-id

Use **dhcp relay information remote-id** to configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Use **undo dhcp relay information remote-id** to restore the default.

Syntax

dhcp relay information remote-id { { **ap-mac** | **ap-mac-ssid** | **normal** } [**format** { **ascii** | **hex** }] | **ap-name** | **ap-name-ssid** | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

ap-mac: Specifies to pad the Remote ID sub-option with the MAC address of an AP.

ap-mac-ssid: Specifies to pad the Remote ID sub-option with the MAC address and SSID of an AP, which are separated by the colon (:). For more information about the SSID, see WLAN client access control in *WLAN Access Configuration Guide*.

normal: Specifies the normal mode in which the padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

ap-name: Specifies to pad the Remote ID sub-option with the name of an AP. For more information about AP names, see AP management in *AP and WT Management Configuration Guide*.

ap-name-ssid: Specifies to pad the Remote ID sub-option with the name and SSID of an AP, which are separated by the colon (:).

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the content of the Remote ID sub-option. You can set the device name by using the **sysname** command.

Usage guidelines

The padding format is always ASCII for the AP name (**ap-name**), AP name and SSID (**ap-name-ssid**), the specified character string (**string**), and the device name (**sysname**).

The padding format for the AP MAC address (**ap-mac**), AP MAC address and SSID (**ap-mac-ssid**), and the **normal** mode is determined by the command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the padding content for the Remote ID sub-option of Option 82 as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information remote-id string device001
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information strategy

Use **dhcp relay information strategy** to configure the strategy for the DHCP relay agent to handle messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Default

The handling strategy for messages that contain Option 82 is **replace**.

Views

Interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82 messages.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the original Option 82 with the configured Option 82 before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

For DHCP requests that do not contain Option 82, the DHCP relay agent always adds Option 82 to the requests before forwarding the requests to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure any padding mode or padding format. The settings do not take effect even if you configure them.

Examples

Specify the handling strategy for Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy keep
```

Related commands

dhcp relay information enable

display dhcp relay information

dhcp relay release ip

Use **dhcp relay release ip** to release a client IP address.

Syntax

dhcp relay release ip *ip-address*

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be released.

Usage guidelines

After you execute this command, the relay agent sends a DHCP-RELEASE packet to the DHCP server and removes the relay entry of the IP address. Upon receiving the packet, the server removes binding information about the specified IP address to release the IP address.

Examples

Release IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay server-address

Use **dhcp relay server-address** to specify DHCP servers on the DHCP relay agent.

Use **undo dhcp relay server-address** to remove DHCP servers.

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

Default

No DHCP server is specified on the DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a DHCP server. The DHCP relay agent forwards DHCP packets received from DHCP clients to this DHCP server.

Usage guidelines

The specified IP address of the DHCP server must not reside on the same subnet as the IP address of the DHCP relay agent interface. Otherwise, the DHCP clients might fail to obtain IP addresses.

You can specify a maximum of eight DHCP servers on an interface. After receiving a DHCP request, the DHCP relay agent forwards the packets to all the specified DHCP servers.

If you do not specify an IP address, the **undo dhcp relay server-address** command removes all DHCP servers on the interface.

Examples

Specify DHCP server address 1.1.1.1 on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay server-address 1.1.1.1
```

Related commands

dhcp select relay

display dhcp relay interface

dhcp relay source-address

Use **dhcp relay source-address** to specify the source IP address for relayed DHCP requests.

Use **undo dhcp relay source-address** to restore the default.

Syntax

dhcp relay source-address { *ip-address* | **gateway** | **relay-interface** }

undo dhcp relay source-address

Default

The relay agent chooses the default source IP address for relayed requests depending on whether its server-side interface and the DHCP server belong to the same VPN instance:

- If they belong to the same VPN instance, the relay agent uses the IP address of the output interface for relayed requests as the default source IP address.
- If they belong to different VPN instances, the relay agent uses the lowest IP address that is in the same VPN instance as the DHCP server as the default source address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address.

gateway: Uses the IP address in the **giaddr** field as the source IP address of the relayed DHCP requests. If the **giaddr** field is empty, the relay agent follows the default rule to specify the source IP address for relayed DHCP requests.

relay-interface: Uses the primary IP address of the relay interface as the source IP address. If this interface does not have an IP address, the relay agent follows the default rule to specify the source IP address for relayed DHCP requests.

Usage guidelines

This command is required if multiple relay interfaces share the same IP address or if a relay interface does not have routes to DHCP servers. You can use this command to specify the IP address of another interface, typically the loopback interface, on the DHCP relay agent as the source IP address for DHCP requests. The relay interface inserts the source IP address in the source IP address field as well as the **giaddr** field in DHCP requests.

If multiple relay interfaces share the same IP address, you must also configure the relay interface to support Option 82. Upon receiving a DHCP request, the relay interface inserts the subnet information in sub-option 5 in Option 82. The DHCP server assigns an IP address according to sub-option 5. The DHCP relay agent looks up the output interface in the MAC address table to forward the DHCP reply.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 1.1.1.1 as the source IP address for relayed DHCP requests on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay source-address 1.1.1.1
```

Related commands

dhcp select relay

dhcp smart-relay enable

Use **dhcp smart-relay enable** to enable the DHCP smart relay feature.

Use **undo dhcp smart-relay enable** to disable the DHCP smart relay feature.

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

Default

The DHCP smart relay feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The smart relay feature allows the relay agent to use secondary IP addresses as the gateway address when the DHCP server does not reply the DHCP-OFFER message. The relay agent initially inserts its primary IP address in the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is returned after two retries, the relay agent switches to secondary IP addresses.

Without this feature, the relay agent always uses the primary IP address as the gateway address.

Examples

Enable the DHCP smart relay feature.

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

Related commands

dhcp select

gateway-list

display dhcp relay check mac-address

Use **display dhcp relay check mac-address** to display MAC address check entries on the relay agent.

Syntax

display dhcp relay check mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display MAC address check entries on the DHCP relay agent.

```
<Sysname> display dhcp relay check mac-address
Source-MAC        Interface                Aging-time
23f3-1122-adf1    Vlan2                    10
23f3-1122-2230    Vlan3                    30
```

Table 9 Command output

Field	Description
Source MAC	Source MAC address of the attacker.
Interface	Interface where the attack comes from.
Aging-time	Aging time of the MAC address check entry, in seconds.

display dhcp relay client-information

Use **display dhcp relay client-information** to display relay entries on the relay agent.

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays relay entries on the specified interface. If you do not specify an interface, this command displays relay entries on all interfaces.

ip *ip-address*: Displays the relay entry for the specified IP address. If you do not specify an IP address, this command displays relay entries for all IP addresses.

Usage guidelines

The DHCP relay agent records relay entries only after you configure the **dhcp relay client-information record** command.

Examples

Display all relay entries on the relay agent.

```
<Sysname> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address       MAC address      Type        Interface           VPN name
10.1.1.1         00e0-0000-0001   Dynamic     Vlan2               N/A
10.1.1.5         00e0-0000-0000   Temporary   Vlan2               N/A
```

Table 10 Command output

Field	Description
Total number of client-information items	Total number of relay entries.
Total number of dynamic items	Total number of dynamic relay entries.
Total number of temporary items	Total number of temporary relay entries.
IP address	IP address of the DHCP client.
MAC address	MAC address of the DHCP client.
Type	Relay entry type: • **Dynamic**—The relay agent creates a dynamic relay entry upon receiving an ACK response from the DHCP server. • **Temporary**—The relay agent creates a temporary relay entry upon receiving a REQUEST packet from a DHCP client.
Interface	Layer 3 interface connected to the DHCP client. **N/A** is displayed for relay entries without interface information.
VPN name	This field is not supported in the current software version. Name of the VPN instance to which the DHCP client belongs. If the DHCP client does not belong to any VPN, this field displays **N/A**.

Related commands

dhcp relay client-information record

reset dhcp relay client-information

display dhcp relay information

Use **display dhcp relay information** to display Option 82 configuration information for the DHCP relay agent.

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays Option 82 configuration information for the specified interface. If you do not specify an interface, this command displays Option 82 configuration information about all interfaces.

Examples

Display Option 82 configuration information for all interfaces.

```
<Sysname> display dhcp relay information
Interface: Vlan-interface100
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Verbose
   Remote ID Pattern: Sysname
   Circuit ID format-type: Undefined
   Remote ID format-type: ASCII
   Node identifier: aabbcc
Interface: Vlan-interface200
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: User Defined
   Remote ID Pattern: User Defined
   Circuit ID format-type: ASCII
   Remote ID format-type: ASCII
   User defined:
   Circuit ID: vlan100
   Remote ID: device001
```

Table 11 Command output

Field	Description
Interface	Interface name.
Status	Option 82 states: • **Enable**—DHCP relay agent support for Option 82 is enabled. • **Disable**—DHCP relay agent support for Option 82 is disabled.
Strategy	Handling strategy for request messages containing Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID Pattern	Padding content mode of the Circuit ID sub-option, **Verbose**, **Normal**, or **User Defined**.
Remote ID Pattern	Padding content mode of the Remote ID sub-option: **Sysname**, **Normal**, **AP-MAC**, **AP-MAC-ssid**, **AP-name**, **AP-name-ssid**,or **User Defined**.
Circuit ID format-type	Padding format of the Circuit ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Remote ID format-type	Padding format of the Remote ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-options.

Field	Description
Circuit ID	User-defined content of the Circuit ID sub-option.
Remote ID	User-defined content of the Remote ID sub-option.

display dhcp relay server-address

Use **display dhcp relay server-address** to display DHCP server addresses configured on an interface.

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP server addresses on the specified interface. If you do not specify an interface, this command displays DHCP server addresses on all interfaces.

Examples

Display DHCP server addresses on all interfaces.

```
<Sysname> display dhcp relay server-address
Interface name                Server IP address
Vlan2                         2.2.2.2
Vlan2                         2.2.2.3
```

Table 12 Command output

Field	Description
Interface name	Interface name.
Server IP address	DHCP server IP address.

Related commands

dhcp relay server-address

display dhcp relay statistics

Use **display dhcp relay statistics** to display DHCP packet statistics on the DHCP relay agent.

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP packet statistics on the specified interface. If you do not specify an interface, this command displays all DHCP packet statistics on the DHCP relay agent.

Examples

Display all DHCP packet statistics on the DHCP relay agent.

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                  0
DHCP packets received from clients:    0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
```

```
DHCPNAK:                        0
BOOTPREPLY:                     0
```

Related commands

reset dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCP clients in a DHCP address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCP address pool.

Syntax

gateway-list *ip-address*&<1-64> [**export-route**]

undo gateway-list [*ip-address*&<1-64>] [**export-route**]

Default

No gateway address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 addresses.

export-route: Binds the gateways to the device's MAC address in the address management module. The ARP module will use the entries to reply to ARP requests from the DHCP clients. If you do not specify this keyword, the gateways will not be bound to the device's MAC address.

Usage guidelines

DHCP clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IP address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCP address pool and bind the gateway addresses to the device's MAC address.

Upon receiving a DHCP DISCOVER or REQUEST from a client that matches a DHCP address pool, the relay agent processes the packet as follows:

1. Fills the **giaddr** field of the packet with the specified gateway address.
2. Forwards the packet to all DHCP servers in the matching DHCP address pool.

The DHCP servers select a DHCP address pool according to the gateway address.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

dhcp smart-relay enable

remote-server

Use **remote-server** to specify DHCP servers for a DHCP relay address pool.

Use **undo remote-server** to remove DHCP servers from a DHCP relay address pool.

Syntax

remote-server *ip-address*&<1-8>

undo remote-server [*ip-address*&<1-8>]

Default

No DHCP server is specified for the DHCP relay address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DHCP server addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify a DHCP server address, the **undo remote-server** command removes all DHCP servers in the DHCP address pool.

Examples

Specify DHCP server 10.1.1.1 for DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server 10.1.1.1
```

reset dhcp relay client-information

Use **reset dhcp relay client-information** to clear relay entries on the DHCP relay agent.

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears relay entries on the specified interface. If you do not specify an interface, this command clears relay entries on all interfaces.

ip *ip-address*: Clears the relay entry for the specified IP address. If you do not specify an IP address, this command clears relay entries for all IP addresses.

Examples

Clear all relay entries on the DHCP relay agent.

```
<Sysname> reset dhcp relay client-information
```

Related commands

display dhcp relay client-information

reset dhcp relay statistics

Use **reset dhcp relay statistics** to clear relay agent statistics.

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCP relay agent statistics.

Examples

Clear all DHCP relay agent statistics.

```
<Sysname> reset dhcp relay statistics
```

Related commands

display dhcp relay statistics

DHCP client commands

dhcp client dad enable

Use **dhcp client dad enable** to enable duplicate address detection.

Use **undo dhcp client dad enable** to disable duplicate address detection.

Syntax

dhcp client dad enable

undo dhcp client dad enable

Default

Duplicate address detection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP client detects IP address conflict through ARP packets. An attacker can act as the IP address owner to send an ARP reply. This makes the client unable to use the IP address assigned by the server. As a best practice, disable duplicate address detection when ARP attacks exist on the network.

Examples

Disable the duplicate address.

```
<Sysname> system-view
[Sysname] undo dhcp client dad enable
```

dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP client.

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

dhcp client identifier

Use **dhcp client identifier** to configure a DHCP client ID for an interface.

Use **undo dhcp client identifier** to restore the default.

Syntax

dhcp client identifier { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo dhcp client identifier

Default

An interface generates the DHCP client ID based on its MAC address. If the interface has no MAC address, it uses the MAC address of the first Ethernet interface to generate its client ID.

Views

Interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the client ID.

hex *hex-string*: Specifies a hexadecimal number of 4 to 64 characters as the client ID.

mac *interface-type interface-number*: Uses the MAC address of the specified interface as a DHCP client ID. The *interface-type interface-number* argument specifies an interface by its type and number.

Usage guidelines

A DHCP client ID is added to the DHCP option 61. A DHCP server can specify IP addresses for clients based on the DHCP client ID. You can specify a DHCP client ID by performing one of the following operations:

- Naming an ASCII string or hexadecimal number as the client ID.
- Using the MAC address of an interface to generate a client ID.

Whichever method you use, make sure the IDs for different DHCP clients are unique.

Examples

Use a hexadecimal number of FFFFFFFF as the client ID for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client identifier hex FFFFFFFF
```

Related commands

display dhcp client

display dhcp client

Use **display dhcp client** to display DHCP client information.

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed DHCP client information. If you do not specify this keyword, the command displays brief DHCP client information.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCP client information on all interfaces.

Examples

Display brief DHCP client information on all interfaces.

```
<Sysname> display dhcp client
Vlan-interface10 DHCP client information:
 Current 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 detailed DHCP client information on all interfaces.

```
<Sysname> display dhcp client verbose
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
   URL: http://192.168.1.1:7547/acs
   Username: bims
   Password: ******
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan10
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 13 Command output

Field	Description
Vlan-interface10 DHCP client information	Information about the interface that acts as the DHCP client.
Current state	Current state of the DHCP client: • **HALT**—The client stops applying for an IP address.

Field	Description
	• **INIT**—The initialization state. • **SELECTING**—The client has sent out a DHCP-DISCOVER message in search for a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—The client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—The client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—The T1 timer expires. • **REBOUNDING**—The T2 timer expires.
Allocated IP	IP address allocated by the DHCP server.
Allocated lease	Allocated lease time.
T1	1/2 lease time (in seconds) of the DHCP client IP address.
T2	7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	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	Gateway address assigned to the client.
Classless static routes	Classless static routes assigned to the client.
Static routes	Classful static routes assigned to the client.
DNS servers	DNS server address assigned to the client.
Domain name	Domain name suffix assigned to the client.
Boot servers	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
ACS parameter	Parameters about the ACS.
URL	URL of the ACS.
Username	Username for logging in to the ACS.
Password	Password for logging in to the ACS. If a password is configured, this field displays **********. If no password is configured, this field is not displayed.
Client ID type	DHCP client ID type: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of a specific interface is used as the client ID value, the type value is 01. • If a hexadecimal number is used as the client ID value, the type value is the first two characters in the string.
Client ID value	Value of the DHCP client ID.
Client ID (with type) hex	DHCP client ID with the type field, a hexadecimal number.
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

Related commands

dhcp client identifier

ip address dhcp-alloc

ip address dhcp-alloc

Use **ip address dhcp-alloc** to configure an interface to use DHCP for IP address acquisition.

Use **undo ip address dhcp-alloc** to cancel an interface from using DHCP.

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

Default

An interface does not use DHCP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When you execute the **undo ip address dhcp-alloc** command, the interface sends a DHCP-RELEASE message to release the IP address obtained through DHCP. If the interface is down, the message cannot be sent out. This situation can occur when a subinterface obtained an IP address through DHCP, and the **shutdown** command is executed on its primary interface. The subinterface will fail to send a DHCP-RELEASE message.

Examples

Configure VLAN-interface 10 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address dhcp-alloc
```

DHCP snooping commands

DHCP snooping works between the DHCP client and the DHCP server or between the DHCP client and the relay agent. DHCP snooping does not work between the DHCP server and the DHCP relay agent.

dhcp snooping binding database filename

Use **dhcp snooping binding database filename** to configure the DHCP snooping device to back up DHCP snooping entries to a file.

Use **undo dhcp snooping binding database filename** to restore the default.

Syntax

dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo dhcp snooping binding database filename

Default

The DHCP snooping device does not back up DHCP snooping entries.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file, a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL. Supported path format type varies by server.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

This command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCP snooping device backs up DHCP snooping entries immediately and runs auto backup. The DHCP snooping device, by default, waits 300 seconds after a DHCP snooping entry change to update the backup file. To change the waiting period, use the **dhcp snooping binding database update interval** command. If no DHCP snooping entry changes, the backup file is not updated.

As a best practice, back up the DHCP snooping entries to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCP snooping device to malfunction.

When the file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.

If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.

- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp**.

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

```
[Sysname] dhcp snooping binding database filename database.dhcp
```

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename url ftp://10.1.1.1/database.dhcp
username 1 password simple 1
```

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp** in the working directory of the TFTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename tftp://10.1.1.1/database.dhcp
```

Related commands

dhcp snooping binding database update interval

dhcp snooping binding database update interval

Use **dhcp snooping binding database update interval** to set the waiting time for the DHCP snooping device to update the backup file after a DHCP snooping entry change.

Use **undo dhcp snooping binding database update interval** to restore the default.

Syntax

dhcp snooping binding database update interval *interval*

undo dhcp snooping binding database update interval

Default

The DHCP snooping device waits 300 seconds to update the backup file after a DHCP snooping entry change. If no DHCP snooping entry changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the waiting time in seconds, in the range of 60 to 864000.

Usage guidelines

When a DHCP snooping entry is learned, updated, or removed, the waiting period starts. The DHCP snooping device updates the backup file when the waiting period is reached. All changed entries during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCP snooping entry auto backup by using the **dhcp snooping binding database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCP snooping device to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update interval 600
```

Related commands

dhcp snooping binding database filename

dhcp snooping binding database update now

Use **dhcp snooping binding database update now** to manually save DHCP snooping entries to the backup file.

Syntax

dhcp snooping binding database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCP snooping entries are saved to the backup file.

This command takes effect only after you configure the DHCP snooping auto backup by using the **dhcp snooping binding database filename** command.

Examples

Manually save DHCP snooping entries to the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update now
```

Related commands

dhcp snooping binding database filename

dhcp snooping check mac-address

Use **dhcp snooping check mac-address** to enable MAC address check for DHCP snooping.

Use **undo dhcp snooping check mac-address** to disable MAC address check for DHCP snooping.

Syntax

dhcp snooping check mac-address

undo dhcp snooping check mac-address

Default

MAC address check for DHCP snooping is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

With MAC address check enabled, DHCP snooping compares the **chaddr** field of a received DHCP request with the source MAC address field in the frame header. If they are the same, DHCP snooping considers this request valid and forwards it to the DHCP server. If they are not the same, DHCP snooping discards the DHCP request.

Examples

Enable MAC address check for DHCP snooping.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping check mac-address
```

dhcp snooping deny

Use **dhcp snooping deny** to configure a port as DHCP packet blocking port.

Use **undo dhcp snooping deny** to restore the default.

Syntax

dhcp snooping deny

undo dhcp snooping deny

Default

A port does not block DHCP requests.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

To avoid IP address acquisition failure, configure a port to block DHCP packets only if no DHCP clients are attached to it.

To enable a port on the snooping device to drop all incoming DHCP requests, configure that port as a DHCP packet blocking port.

Examples

Configure GigabitEthernet 1/0/1 as a DHCP packet blocking port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping deny
```

dhcp snooping enable

Use **dhcp snooping enable** to enable DHCP snooping.

Use **undo dhcp snooping enable** to disable DHCP snooping.

Syntax

dhcp snooping enable

undo dhcp snooping enable

Default

DHCP snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable DHCP snooping on the device, trusted ports forward responses from DHCP servers and untrusted ports discard responses. This mechanism ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

When DHCP snooping is disabled, all ports on the device can forward responses from DHCP servers.

Examples

Enable DHCP snooping.

```
<Sysname> system-view
[Sysname] dhcp snooping enable
```

dhcp snooping information circuit-id

Use **dhcp snooping information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option.

Use **undo dhcp snooping information circuit-id** to restore the default.

Syntax

In Layer 2 Ethernet interface view/Layer 2 aggregate interface view:

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

In service template view:

dhcp snooping information circuit-id { **normal** | **wlan-private** } [**format** { **ascii** | **hex** }]

undo dhcp snooping information circuit-id

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Service template view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Circuit ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Circuit ID sub-option for packets received from the default VLAN.

string *circuit-id*: Specifies the string mode, in which the padding content for the Circuit ID sub-option is a case-sensitive string of 3 to 63 characters.

normal: Specifies the normal mode. The padding content includes the VLAN ID and interface number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format.

  NOTE:

  If the **sysname** keyword is specified, do not include any spaces when you set the device name. Otherwise, the DHCP snooping device fails to add or replace Option 82.

- **user-defined** *node-identifier*: Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

wlan-private: Specifies the wlan-private mode. The padding content includes "**WLAN**", interface name, VLAN ID, SSID, BSSID, host name, and AP MAC address.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 14 shows how the padding format is determined for different modes.

Table 14 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is always ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.
wlan-private	ASCII.	ASCII.	ASCII for "**WLAN**", interface name, SSID, and host name. Hex for VLAN ID, BSSID, and AP MAC address.

You can configure the padding mode and padding format for the Circuit ID sub-option for APs in the following views:

- AP view (on ACs).
- Layer 2 Ethernet interface view.
- Layer 2 aggregate interface view.
- Service template view.

The configuration in Layer 2 interface view takes precedence over that in service template view, and the configuration in AP view has the lowest priority.

For more information about Circuit ID sub-option configuration on ACs in AP view, see AP management configuraiton in *WLAN Configuration Guide*.

Examples

In Layer 2 Ethernet interface view, configure verbose as the padding mode, device name as the node identifier, and ASCII as the padding format for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose
node-identifier sysname format ascii
```

In service template view, configure normal as the padding mode and ASCII as the padding format for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] service-template enable
[Sysname-wlan-st-service1] dhcp snooping information circuit-id normal format ascii
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

dhcp snooping information enable

Use **dhcp snooping information enable** to enable DHCP snooping to support Option 82.

Use **undo dhcp snooping information enable** to disable this feature.

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

Default

DHCP snooping does not support Option 82.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Service template view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping to add Option 82 into DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp snooping information circuit-id** and **dhcp snooping information remote-id** commands. If the received DHCP request packets contain Option 82, DHCP snooping handles the packets according to the strategy configured by the **dhcp snooping information strategy** command.

Examples

In Layer 2 Ethernet interface view, enable DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
```

In service template view, enable DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] service-template enable
[Sysname-wlan-st-service1] dhcp snooping information enable
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

dhcp snooping information strategy

dhcp snooping information remote-id

Use **dhcp snooping information remote-id** to configure the padding mode and padding format for the Remote ID sub-option.

Use **undo dhcp snooping information remote-id** to restore the default.

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Remote ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Remote ID sub-option for packets received from the default VLAN.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the Remote ID sub-option. You can configure the device name by using the **sysname** command in system view.

normal: Specifies the normal mode. The padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

DHCP snooping uses ASCII to pad the specified string or device name for the Remote ID sub-option. The padding format for the normal padding mode is determined by the command configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Pad the Remote ID sub-option with a character string of **device001**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

dhcp snooping information strategy

Use **dhcp snooping information strategy** to configure the handling strategy for Option 82 in request messages.

Use **undo dhcp snooping information strategy** to restore the default.

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Default

The handling strategy for Option 82 in request messages is **replace**.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the Option 82 with the configured Option 82 before forwarding the DHCP messages. If the DHCP messages do not carry Option 82, the device adds Option 82 according to the padding configuration before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82. For DHCP requests that do not contain Option 82, the DHCP snooping device always adds Option 82 into the requests before forwarding them to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and a padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure a padding mode or padding format for Option 82.

Examples

Specify the handling strategy for Option 82 in request messages as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

dhcp snooping log enable

Use **dhcp snooping log enable** to enable DHCP snooping logging.

Use **undo dhcp snooping log enable** to disable DHCP snooping logging.

Syntax

dhcp snooping log enable

undo dhcp snooping log enable

Default

DHCP snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP snooping device to generate DHCP snooping logs and send them to the information center. The information helps administrators locate and solve problems. For

information about the log destination and output rule configuration in the information center, see *System Management Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Examples

Enable DHCP snooping logging.

```
<Sysname> system-view
[Sysname] dhcp snooping log enable
```

dhcp snooping max-learning-num

Use **dhcp snooping max-learning-num** to set the maximum number of DHCP snooping entries that an interface can learn.

Use **undo dhcp snooping max-learning-num** to restore the default.

Syntax

dhcp snooping max-learning-num *max-number*

undo dhcp snooping max-learning-num

Default

The maximum number of DHCP snooping entries for an interface to learn is unlimited.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of DHCP snooping entries for an interface to learn. The value range for this argument is 1 to 4294967295.

Usage guidelines

When an interface learns the maximum number of DHCP snooping entries, the interface stops learning DHCP snooping entries. This does not affect the operating of the DHCP snooping feature.

Examples

Allow Layer 2 Ethernet interface GigabitEthernet 1/0/1 to learn a maximum of 10 DHCP snooping entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping max-learning-num 10
```

dhcp snooping rate-limit

Use **dhcp snooping rate-limit** to enable DHCP snooping packet rate limit on an interface and set the limit value.

Use **undo dhcp snooping rate-limit** to disable DHCP snooping packet rate limit.

Syntax

dhcp snooping rate-limit *rate*

undo dhcp snooping rate-limit

Default

The DHCP snooping packet rate limit is disabled on an interface.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the maximum rate in Kbps. The value range for this argument is 64 to 512.

Usage guidelines

This command takes effect only when DHCP snooping is enabled.

With the rate limit feature, the interface discards DHCP packets that exceed the maximum rate.

The rate configured on a Layer 2 aggregate interface applies to all members of the aggregate interface. If a member interface leaves the aggregation group, it uses the rate configured in its Ethernet interface view.

Examples

Set the maximum rate to 64 Kbps at which Layer 2 Ethernet interface GigabitEthernet 1/0/1 can receive DHCP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping rate-limit 64
```

dhcp snooping trust

Use **dhcp snooping trust** to configure a port as a trusted port.

Use **undo dhcp snooping trust** to restore the default state of a port.

Syntax

dhcp snooping trust

undo dhcp snooping trust

Default

After you enable DHCP snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Specify the ports facing the DHCP server as trusted ports and specify the other ports as untrusted ports so DHCP clients can obtain valid IP addresses.

Examples

Specify Layer 2 Ethernet interface GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping trust
```

Related commands

display dhcp snooping trust

display dhcp snooping binding

Use **display dhcp snooping binding** to display DHCP snooping entries.

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Specifies the VLAN ID where the IP address resides.

verbose: Displays detailed information about DHCP snooping entries. If you do not specify this keyword, the command displays brief information about DHCP snooping entries.

Usage guidelines

If you do not specify any parameters, this command displays all DHCP snooping entries.

Examples

Display information about all DHCP snooping entries.

```
<Sysname> display dhcp snooping binding
 2 DHCP snooping entries found
 IP address      MAC address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 1.1.1.7         0000-0101-0107 16907533     2     3     GE1/0/1
 1.1.1.11        0000-0101-010b 16907537     2     3     GE1/0/3
```

Display detailed information about DHCP snooping entries.

```
<Sysname> display dhcp snooping binding verbose
 IP address: 1.1.1.7
 MAC address: 0000-0101-0107
 Lease: 16907553 seconds
 VLAN: 2
 SVLAN: 3
 Interface: GigabitEthernet1/0/1
 Client Identifier: N/A
 Authorized Client Identifier: N/A

 IP address: 1.1.1.104
 MAC address: 0000-0101-010b
 Lease: 16907537 seconds
 VLAN: 2
 SVLAN: 3
```

```
Interface: GigabitEthernet1/0/3
Client Identifier: N/A
Authorized Client Identifier: N/A
```

Table 15 Command output

Field	Description
DHCP snooping entries found	Number of DHCP snooping entries.
IP address	IP address assigned to the DHCP client.
MAC address	MAC address of the DHCP client.
Lease	Remaining lease duration in seconds.
VLAN	When the DHCP packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCP client resides.
SVLAN	When the DHCP packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connected to the DHCP client.
Client Identifier	Client ID in the entry.
Authorized Client Identifier	Authorized client ID in the entry.

Related commands

dhcp snooping enable

reset dhcp snooping binding

display dhcp snooping binding database

Use **display dhcp snooping binding database** to display information about DHCP snooping entry auto backup.

Syntax

display dhcp snooping binding database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCP snooping entry auto backup.

```
<Sysname> display dhcp snooping binding database
File name               :   database.dhcp
Username                :
Password                :
Update interval         :   600 seconds
Latest write time       :   Feb 27 18:48:04 2012
Status                  :   Last write succeeded.
```

Table 16 Command output

Field	Description
File name	Name of the DHCP snooping entry backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCP snooping entry change for the DHCP snooping device to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp snooping information

Use **display dhcp snooping information** to display Option 82 configuration on the DHCP snooping device.

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays Option 82 configuration on all Layer 2 Ethernet interfaces.

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

Examples

Display Option 82 configuration on all interfaces.

```
<Sysname> display dhcp snooping information all
Interface: Bridge-Aggregation1
   Status: Disable
   Strategy: Drop
   Circuit ID:
     Padding format: User Defined
       User defined: abcd
     Format: ASCII
   Remote ID:
     Padding format: Normal
     Format: ASCII
```

```
VLAN 10:
  Circuit ID: abcd
  Remote ID: company
```

Table 17 Command output

Field	Description
Interface	Interface name.
Status	Option 82 status, **Enable** or **Disable**.
Strategy	Handling strategy for DHCP requests that contain Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID	Content of the Circuit ID sub-option.
Padding format	Padding format of Option 82: • For Circuit ID sub-option, the padding format can be **Normal**, **User Defined**, **Verbose (sysname)**, **Verbose (MAC)**, or **Verbose (user defined)**. • For Remote ID sub-option, the padding format can be **Normal**, **Sysname**, or **User Defined**.
Node identifier	Access node identifier. For the Circuit ID and Remote ID sub-options, this field displays the user-defined node identifier.
User defined	Content of the user-defined sub-option.
Format	Code type of Option 82 sub-option: • For Circuit ID sub-option, the code type can be **ASCII**, **Default**, or **Hex**. • For Remote ID sub-option, the code type can be **ASCII** or **Hex**.
Remote ID	Content of the Remote ID sub-option.
VLAN	Pads Circuit ID and Remote ID sub-options in the DHCP packets received in the specified VLAN.

display dhcp snooping packet statistics

Use **display dhcp snooping packet statistics** to display DHCP packet statistics for DHCP snooping.

Syntax

In standalone mode:

display dhcp snooping packet statistics

In IRF mode:

display dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DHCP packet statistics for the master device. (In IRF mode.)

Examples

Display DHCP packet statistics for DHCP snooping.

```
<Sysname> display dhcp snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Invalid DHCP packets dropped           : 0
```

Related commands

reset dhcp snooping packet statistics

display dhcp snooping trust

Use **display dhcp snooping trust** to display information about trusted ports.

Syntax

display dhcp snooping trust

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
DHCP snooping is enabled.
 Interface                                      Trusted
 ========================                       ============
 GigabitEthernet1/0/1                           Trusted
```

Table 18 Command output

Field	Description
Interface	Interface name.
Trusted	The port is a trusted port.

Related commands

dhcp snooping trust

reset dhcp snooping binding

Use **reset dhcp snooping binding** to clear DHCP snooping entries.

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Clears DHCP snooping entries for the specified VLAN. If you do not specify a VLAN, this command clears DHCP snooping entries for the default VLAN.

Examples

Clear all DHCP snooping entries.

```
<Sysname> reset dhcp snooping binding all
```

Related commands

display dhcp snooping binding

reset dhcp snooping packet statistics

Use **reset dhcp snooping packet statistics** to clear DHCP packet statistics for DHCP snooping.

Syntax

In standalone mode:

reset dhcp snooping packet statistics

In IRF mode:

reset dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears DHCP packet statistics for the master device. (In IRF mode.)

Examples

Clear DHCP packet statistics for DHCP snooping.

```
<Sysname> reset dhcp snooping packet statistics
```

Related commands

display dhcp snooping packet statistics

BOOTP client commands

display bootp client

Use **display bootp client** to display information about a BOOTP client.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays BOOTP client information on all interfaces.

Examples

Display BOOTP client information on VLAN-interface 10.

```
<Sysname> display bootp client interface vlan-interface 10
Vlan-interface10 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 00e0-fc0a-c3ef
```

Table 19 Command output

Field	Description
Vlan-interface10 BOOTP client information	Information about the interface that acts as a BOOTP client.
Allocated IP	BOOTP client's IP address allocated by the BOOTP server.
Transaction ID	Value of the **XID** field in a BOOTP message. The BOOTP client chooses a random number for the **XID** field when sending a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client drops the BOOTP response.
Mac Address	MAC address of a BOOTP client.

Related commands

ip address bootp-alloc

ip address bootp-alloc

Use **ip address bootp-alloc** to configure an interface to use BOOTP for IP address acquisition.

Use **undo ip address bootp-alloc** to cancel an interface from using BOOTP.

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

Default

An interface does not use BOOTP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Examples

Configure VLAN-interface 10 to use BOOTP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address bootp-alloc
```

Related commands

`display bootp client`

Contents

Loop detection commands 1
display loopback-detection 1
loopback-detection action 1
loopback-detection enable 3
loopback-detection global action 3
loopback-detection global enable 4
loopback-detection interval-time 5

Loop detection commands

display loopback-detection

Use **display loopback-detection** to display the loop detection configuration and status.

Syntax

display loopback-detection

Views

Any view

Predefined user roles

network-admin

network-operator

Example

Display the loop detection configuration and status.

```
<Sysname> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
 Interface               Action mode
 GigabitEthernet1/0/3    None
```

Table 1 Command output

Field	Description
Action mode	Loop protection action: • **Block**—When a loop is detected on a port, the device performs the following operations: ○ Logs the event. ○ Disables the port from learning MAC addresses. ○ Blocks the port. • **None**—When a loop is detected on a port, the device logs the event without taking any action on the port. • **No-learning**—When a loop is detected on a port, the device logs the event and disables the port from learning MAC addresses. • **Shutdown**—When a loop is detected on a port, the device performs the following operations: ○ Logs the event. ○ Shuts down the port to disable it from receiving or sending frames. The device automatically sets the port to the forwarding state after a time interval. Set the time interval by using the **shutdown-interval** command (see *System Management Command Reference*).

loopback-detection action

Use **loopback-detection action** to set the loop protection action on a per-port basis.

Use **undo loopback-detection action** to restore the default.

Syntax

In Layer 2 Ethernet interface view:

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

In Layer 2 aggregate interface view:

loopback-detection action shutdown

undo loopback-detection action

Default

When the device detects a loop on a port, it logs the event without taking any action on the port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

block: Enables the block mode. If a loop is detected, the device performs the following operations:

- Logs the event.
- Disables MAC address learning.
- Blocks the port.

Layer 2 aggregate interfaces do not support this keyword.

no-learning: Enables the no-learning mode. If a loop is detected, the device logs the event and disables MAC address learning on the port. Layer 2 aggregate interfaces do not support this keyword.

shutdown: Enables the shutdown mode. If a loop is detected, the device logs the event and shuts down the port. The device automatically sets the port to the forwarding state after the time interval set by using the **shutdown-interval** command (see *System Management Command Reference*).

Usage guidelines

To set the loop protection action globally, use the **loopback-detection global action** command.

The global action applies to all ports. The per-port action applies to the individual ports. The per-port action takes precedence over the global action.

Example

Set the loop protection action to **shutdown** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

Related commands

display loopback-detection

loopback-detection global action

loopback-detection enable

Use **loopback-detection enable** to enable loop detection on a per-port basis.

Use **undo loopback-detection enable** to disable loop detection on a port.

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is disabled on ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be equal to or greater than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Enable loop detection on GigabitEthernet 1/0/1 for VLAN 10 through VLAN 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection global enable

loopback-detection global action

Use **loopback-detection global action** to set the global loop protection action.

Use **undo loopback-detection global action** to restore the default.

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

Default

When the device detects a loop on a port, it logs the event without taking any action on the port.

Views

System view

Predefined user roles

network-admin

Parameters

shutdown: Enables the shutdown mode. If a loop is detected, the device logs the event and shuts down the port. The device automatically sets the port to the forwarding state after you set the time interval by using the **shutdown-interval** command (see *System Management Command Reference*).

Usage guidelines

To set the loop protection action on a per-port basis, use the **loopback-detection action** command in interface view.

The global action applies to all ports. The per-port action applies to the individual ports. The per-port action takes precedence over the global action.

Example

Set the global loop protection action to **shutdown**.

```
<Sysname> system-view
[System] loopback-detection global action shutdown
```

Related commands

display loopback-detection

loopback-detection action

loopback-detection global enable

Use **loopback-detection global enable** to enable loop detection globally.

Use **undo loopback-detection global enable** to disable loop detection globally.

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is globally disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be equal to or greater than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Globally enable loop detection for VLAN 10 through VLAN 20.

```
<Sysname> system-view
[System] loopback-detection global enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection enable

loopback-detection interval-time

Use **loopback-detection interval-time** to set the loop detection interval.

Use **undo loopback-detection interval-time** to restore the default.

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

Default

The loop detection interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the loop detection interval in the range of 1 to 300 seconds.

Usage guidelines

With loop detection enabled, the device sends loop detection frames at the specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

Example

Set the loop detection interval to 10 seconds.

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

Related commands

display loopback-detection

Contents

Spanning tree commands 1

active region-configuration 1
check region-configuration 1
display stp 3
display stp abnormal-port 9
display stp bpdu-statistics 10
display stp down-port 13
display stp history 13
display stp region-configuration 16
display stp root 17
display stp tc 17
instance 19
region-name 20
reset stp 21
revision-level 21
snmp-agent trap enable stp 22
stp bpdu-protection 23
stp bridge-diameter 24
stp compliance 25
stp config-digest-snooping 25
stp cost 26
stp edged-port 28
stp enable 28
stp global config-digest-snooping 29
stp global enable 30
stp global mcheck 31
stp ignore-pvid-inconsistency 31
stp loop-protection 32
stp max-hops 33
stp mcheck 33
stp mode 34
stp no-agreement-check 35
stp pathcost-standard 36
stp point-to-point 37
stp port priority 38
stp port-log 39
stp priority 40
stp pvst-bpdu-protection 40
stp region-configuration 41
stp role-restriction 42
stp root primary 42
stp root secondary 43
stp root-protection 44
stp tc-protection 45
stp tc-protection threshold 45
stp tc-restriction 46
stp tc-snooping 47
stp timer forward-delay 47
stp timer hello 48
stp timer max-age 49
stp timer-factor 50
stp transmit-limit 51
stp vlan enable 52
vlan-mapping modulo 53

Spanning tree commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

active region-configuration

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

Syntax

active region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

When you configure MST region parameters, MSTP launches a new spanning tree calculation process that might cause network topology instability. This is most likely to occur when you configure the VLAN-to-instance mapping table. The launch occurs after you execute the **active region-configuration** command or the **stp global enable** command.

As a best practice, use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Run this command only when they are correct.

Examples

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

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

Related commands

check region-configuration

instance

region-name

revision-level

stp global enable

vlan-mapping modulo

check region-configuration

Use **check region-configuration** to display MST region pre-configuration information.

Syntax

check region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

Spanning tree devices belong to the same MST region only when they are connected through a physical link and configured with the same details as follows:

- Format selector (0 by default and not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

As a best practice, use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

Examples

Display MST region pre-configurations.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
 Admin Configuration
   Format selector      : 0
   Region name          : 001122334400
   Revision level       : 0
   Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

   Instance  VLANs Mapped
   0         1, 3 to 4094
   15        2
```

Table 1 Command output

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

Related commands

active region-configuration

instance

region-name

revision-level

vlan-mapping modulo

display stp

Use **display stp** to display spanning tree status and statistics.

Syntax

In standalone mode:

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

In IRF mode:

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*.

brief: Displays brief spanning tree status and statistics. If this keyword is not specified, the command displays detailed spanning tree status and statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (In IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port list, this command applies to the specified ports.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN or port, this command applies to all ports in all VLANs.
- If you only specify a VLAN list but not a port, this command applies to all ports in the specified VLANs.
- If you only specify a port list but not a VLAN, this command applies to the specified ports in all VLANs.

- If you specify both a VLAN list and a port list, this command applies to the ports in the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify an MSTI list but not a port, this command applies to all ports in the specified MSTIs.
- If you specify a port list but not an MSTI, this command applies to all MSTIs on the specified ports.
- If you specify both an MSTI list and a port list, this command applies to the specified ports in the specified MSTIs.

Examples

In MSTP mode, display the brief spanning tree status and statistics for MSTI 0 on port GigabitEthernet 1/0/1.

```
<Sysname> display stp instance 0 interface GigabitEthernet 1/0/1 brief
 MST ID      Port                        Role  STP State     Protection
 0           0           GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
```

In PVST mode, display the brief spanning tree status and statistics for VLAN 2 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 brief
 VLAN ID     Port                        Role  STP State     Protection
 2           GigabitEthernet1/0/1        ALTE  DISCARDING    LOOP
```

Table 2 Command output

Field	Description
MST ID	MSTI ID in the MST region.
Port	Port name, corresponding to each MSTI or VLAN.
Role	Port role: • **ALTE**—The port is an alternate port. • **BACK**—The port is a backup port. • **ROOT**—The port is a root port. • **DESI**—The port is a designated port. • **MAST**—The port is a master port. • **DISA**—The port is disabled.
STP State	Spanning tree status on the port: • **FORWARDING**—The port can receive and send BPDUs and also forward user traffic. • **DISCARDING**—The port can receive and send BPDUs but cannot forward user traffic. • **LEARNING**—The port is in a transitional state. It can receive and send BPDUs but cannot forward user traffic.
Protection	Effective spanning tree protection feature on the port: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.

In MSTP mode, display the detailed spanning tree status and statistics for all MSTIs on all ports.

```
<Sysname> display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 32768.0001-0000-0000
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 32768.0001-0000-0000, 0
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 2
 Time since last TC  : 0 days 0h:0m:58s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 32
          TCN: 0, Config: 0, RST: 0, MST: 32
 BPDU received       : 2
          TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
 Bridge ID           : 32768.0001-0000-0000
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 Master bridge       : 32768.0001-0000-0000
 Cost to master      : 0
 TC received         : 0

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
```

```
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 64
 Port times          : RemHops 20
```

In PVST mode, display the spanning tree status and statistics for all ports in all VLANs.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp
-------[VLAN 1 Global Info]-------
Protocol status     : Enabled
Bridge ID           : 32768.000f-e200-2200
Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC     : 0.00e0-fc0e-6554, 200200
RootPort ID         : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

 ----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.153
 Port cost(Legacy)   : Config=auto, Active=200
 Desg. bridge/port   : 32768.000f-e200-2200, 128.2
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : False
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s

-------[VLAN 2 Global Info]-------
Protocol status      : Enabled
Bridge ID            : 32768.000f-e200-2200
Bridge times         : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC      : 0.00e0-fc0e-6554, 200200
RootPort ID          : 128.48
BPDU-Protection      : Disabled
TC or TCN received   : 2
Time since last TC   : 0 days 0h:5m:42s
```

In MSTP mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1s
```

```
 Version            : 3
 Bridge-Prio.       : 32768
 MAC address        : 000f-e200-8048
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 Max hops           : 20
 TC Snooping        : Disabled
```

In PVST mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1w (pvst)
 Version            : 2
 Bridge-Prio.       : 32768
 MAC address        : 3822-d69f-0800
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 TC Snooping        : Disabled
```

Table 3 Command output

Field	Description
Bridge ID	Bridge ID, which contains the device's priority and its MAC address. For example, in output 32768.000f-e200-2200, the value preceding the dot is the device's priority, and the value following the dot is the device's MAC address.
Bridge times	Major parameters for the bridge: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MaxHops**—Maximum hops within the MST region.
Root ID/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
RegRoot ID/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the CIST regional root).
VlanRoot ID/RPC	VLAN root ID and root path cost (the path cost from the device to the VLAN root bridge).
RootPort ID	Root port ID. The value **0.0** indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of the BPDU guard feature.
Bridge Config-Digest-Snooping	Global status of Digest Snooping.
TC or TCN received	Number of TC/TCN BPDUs received in the MSTI or VLAN.
Time since last TC	Time since the latest topology change in the MSTI or VLAN.
Port protocol	Status of the spanning tree feature on the port.
Port role	Port role: • Alternate.

Field	Description
	• Backup. • Root. • Designated. • Master. • Disabled.
(Boundary)	The port is a regional boundary port.
Port cost(Legacy)	Path cost of the port. The field in parentheses indicates the standard (legacy, dot1d-1998, or dot1t) used for port path cost calculation. • **Config**—Configured value. • **Active**—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	The port is an edge port or non-edge port. • **Config**—Configured value. • **Active**—Actual value.
Point-to-Point	The port is connected to a point-to-point link or not. • **Config**—Configured value. • **Active**—Actual value.
Transmit limit	Maximum number of BPDUs sent by a port within each hello time.
Protection type	Whether spanning tree protection is configured on the port: • **Config**—Configured spanning tree protection feature. • **Active**—Effective spanning tree protection feature. Spanning tree protection features are as follows: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. • **PVST BPDU**—PVST BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.
TC-Restriction	Status of TC transmission restriction on the port.
Role-Restriction	Status of port role restriction on the port.
MST BPDU format	Format of the MST BPDUs that the port can send: • **Config**—Configured value (legacy or 802.1s). • **Active**—Actual value (legacy or 802.1s).
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	Indicates whether the port rapidly transits to the forwarding state in the MSTI or VLAN.
Num of VLANs mapped	Number of VLANs that are mapped to the MSTI.
Port times	Major parameters for the port: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer.

Field	Description
	• **FwdDelay**—Forward delay timer. • **MsgAge**—Message age timer. • **RemHops**—Remaining hops.
BPDU sent	Statistics on sent BPDUs.
BPDU received	Statistics on received BPDUs.
RegRoot ID/IRPC	MSTI regional root/internal path cost.
Root Type	MSTI root type: • **Primary root**. • **Secondary root**.
Master bridge	MSTI root bridge ID.
Cost to master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.
Protocol status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	In MSTP mode: Device's priority in the CIST. In PVST mode: Device's priority in VLAN 1.
Max age(s)	Aging timer for BPDUs (in seconds, which is the same as the aging timer for VLAN 1 in PVST mode).
Forward delay(s)	Port state transition delay (in seconds, which is the same as the port state transition delay for VLAN 1 in PVST mode).
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds, which is the same as the interval for VLAN 1 in PVST mode).
Max hops	Maximum hops in the MSTI.
TC Snooping	Status of TC Snooping: **Enabled** or **Disabled**.

Related commands

`reset stp`

display stp abnormal-port

Use **`display stp abnormal-port`** to display information about ports that are blocked by spanning tree protection features.

Syntax

`display stp abnormal-port`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> display stp abnormal-port
 MST ID      Blocked Port                Reason
 1           GigabitEthernet1/0/1        Root-Protected
 2           GigabitEthernet1/0/2        Loop-Protected
 12          GigabitEthernet1/0/3        Loopback-Protected
```

In PVST mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
 VLAN ID      Blocked Port                Reason
 1            GigabitEthernet1/0/1        Root-Protected
 2            GigabitEthernet1/0/2        Loop-Protected
 2            GigabitEthernet1/0/3        Loopback-Protected
```

Table 4 Command output

Field	Description
MST ID	MSTI of a blocked port.
VLAN ID	VLAN of a blocked port.
Blocked Port	Name of a blocked port.
BlockReason	Reason that the port was blocked: • **Root-Protected**—Root guard feature. • **Loop-Protected**—Loop guard feature. • **Loopback-Protected**—Self-loop protection. A port in the MSTI receives a BPDU sent by itself. • **Disputed**—Dispute guard. A port receives a low-priority BPDU from a non-blocked designated port in forwarding or learning state. • **InconsistentPortType-Protected**—Inconsistent port type protection. • **InconsistentPvid-Protected**—Inconsistent PVID protection.

display stp bpdu-statistics

Use **display stp bpdu-statistics** to display the BPDU statistics for ports.

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

Usage guidelines

In MSTP mode, the command output is sorted by port name and by MSTI ID on each port.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify a port but not an MSTI, this command applies to all MSTIs on the port.
- If you specify both an MSTI ID and a port, this command applies to the specified MSTI on the port.

In STP, PVST, or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port, this command applies to the port.

Examples

In MSTP mode, display the BPDU statistics for all MSTIs on GigabitEthernet 1/0/1.

```
<Sysname> display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Instance-Independent:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2          10:33:12 01/13/2011
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4          10:33:11 01/13/2011
 MST received                151        10:37:43 01/13/2011

 Instance 0:
 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 1          10:32:40 01/13/2011
 TC sent                     3          10:33:11 01/13/2011
```

```
 TC received                0
```

In PVST mode, display the BPDU statistics for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Type                       Count      Last Updated
 -------------------------- ---------- -----------------
 Invalid BPDUs              0
 Looped-back BPDUs          0
 Max-aged BPDUs             0
 TCN sent                   0
 TCN received               0
 TCA sent                   0
 TCA received               2           10:33:12 01/13/2010
 Config sent                0
 Config received            0
 RST sent                   0
 RST received               0
 MST sent                   4           10:33:11 01/13/2010
 MST received               151         10:37:43 01/13/2010
 Timeout BPDUs              0
 Max-hoped BPDUs            0
 TC detected                511         10:32:40 01/13/2010
 TC sent                    8844        10:33:11 01/13/2010
 TC received                1426        10:33:32 01/13/2010
 PVID inconsistency BPDUs   0
```

Table 5 Command output

Field	Description
Port	Port name.
Instance-Independent	Statistics not related to a specific MSTI.
Type	Statistical item.
Looped-back BPDUs	Number of BPDUs sent and then received by the same port.
Max-aged BPDUs	Number of BPDUs whose max age was exceeded.
TCN sent	Number of sent TCN BPDUs.
TCN received	Number of received TCN BPDUs.
TCA sent	Number of sent TCA BPDUs.
TCA received	Number of received TCA BPDUs.
Config sent	Number of sent configuration BPDUs.
Config received	Number of received configuration BPDUs.
RST sent	Number of sent RSTP BPDUs.
RST received	Number of received RSTP BPDUs.

Field	Description
MST sent	Number of sent MSTP BPDUs.
MST received	Number of received MSTP BPDUs.
Instance	Statistics for a specific MSTI.
Timeout BPDUs	Number of expired BPDUs.
Max-hoped BPDUs	Number of BPDUs whose maximum hops were exceeded.
TC detected	Number of detected topology changes.
TC sent	Number of sent TC BPDUs.
TC received	Number of received TC BPDUs.
PVID inconsistency BPDUs	Number of received PVST BPDUs with a PVID inconsistent with the incoming port.

display stp down-port

Use **display stp down-port** to display information about ports that were shut down by spanning tree protection features.

Syntax

display stp down-port

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about ports that were shut down by spanning tree protection features.

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

Table 6 Command output

Field	Description
Down Port	Name of a port that was shut down by the spanning tree protection features.
Reason	Reason that the port was shut down: • **BPDU protection**—Indicates the BPDU guard feature. • **PVST BPDU protection**—Indicates the PVST BPDU guard feature.

display stp history

Use **display stp history** to display port role calculation history.

Syntax

In standalone mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history**

In IRF mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (In IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port role calculation time.

In PVST mode, the command output is sorted by VLAN ID and by port role calculation time in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

(In standalone mode.) In MSTP mode, display the port role calculation history for MSTI 2.

```
<Sysname> display stp instance 2 history
 ------------------  Instance 2   ---------------------

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

 Port GigabitEthernet1/0/2
```

```
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
```

(In standalone mode.) In PVST mode, display the port role calculation history for VLAN 2.

```
<Sysname> display stp vlan 2 history
 ------------------  VLAN 2   ---------------------

 Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

(In IRF mode.) In MSTP mode, display the port role calculation history on the specified slot in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
 --------------- STP slot 1 history trace ---------------
 ------------------  Instance 2   ---------------------
Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
```

(In IRF mode.) In PVST mode, display the port role calculation history on the specified slot in VLAN 2.

```
<Sysname> display stp vlan 2 history slot 1
 --------------- STP slot 1 history trace ---------------
 ------------------  VLAN 2   ---------------------

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

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

Table 7 Command output

Field	Description
Port	Port name.
Role change	Role change of the port (**Aged** means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.

display stp region-configuration

Use **`display stp region-configuration`** to display effective MST region configuration.

Syntax

`display stp region-configuration`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display effective MST region configuration.

```
<Sysname> display stp region-configuration
 Oper Configuration
   Format selector      : 0
   Region name          : hello
   Revision level       : 0
   Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

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

Table 8 Command output

Field	Description
Format selector	Format selector that is defined by the spanning tree protocol. The default value is 0, and the selector cannot be configured.
Region name	MST region name.
Revision level	Revision level of the MST region. The default value is 0, and the level can be configured by using the **`revision-level`** command.

Field	Description
VLANs Mapped	VLANs mapped to the MSTI.

Related commands

instance

region-name

revision-level

vlan-mapping modulo

display stp root

Use **display stp root** to display the root bridge information of spanning trees.

Syntax

display stp root

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display the root bridge information of all spanning trees.

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

In PVST mode, display the root bridge information of all spanning trees.

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

Table 9 Command output

Field	Description
ExtPathCost	External path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
IntPathCost	Internal path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
Root Port	Root port name (displayed only if a port of the device is the root port of the MSTI).

display stp tc

Use **display stp tc** to display the incoming and outgoing TC/TCN BPDU statistics for ports.

Syntax

In standalone mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc**

In IRF mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (In IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

(In standalone mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports in MSTI 0.

```
<Sysname> display stp instance 0 tc
 MST ID      Port                      Receive      Send
 0           GigabitEthernet1/0/1      6            4
 0           GigabitEthernet1/0/2      0            2
```

(In standalone mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports in VLAN 2.

```
<Sysname> display stp vlan 2 tc
 VLAN ID     Port                      Receive      Send
 2           GigabitEthernet1/0/1      6            4
 2           GigabitEthernet1/0/2      0            2
```

(In IRF mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
```

```
-------------- STP slot 1 TC or TCN count -------------
MST ID      Port                        Receive      Send
0           GigabitEthernet1/0/1        6            4
0           GigabitEthernet1/0/2        0            2
```

(In IRF mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in VLAN 2.

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

Table 10 Command output

Field	Description
Port	Port name.
Receive	Number of TC/TCN BPDUs received on a port.
Send	Number of TC/TCN BPDUs sent by a port.

instance

Use **instance** to map a list of VLANs to an MSTI.

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

Syntax

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

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

Default

All VLANs are mapped to the CIST.

Views

MST region view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an MSTI ID in the range of 0 to 4094. A value of 0 represents the CIST. The value range for the *instance-id* argument is 1 to 4094 for the **undo instance** command.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

CAUTION:

Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occur.

If you do not specify any VLANs in the **undo instance** command, all VLANs mapped to the specified MSTI are remapped to the CIST.

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

You can configure VLAN-to-instance mapping for up to 65 MSTIs.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Examples

Map VLAN 2 to MSTI 1.

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

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

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

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

Syntax

region-name *name*

undo region-name

Default

The MST region name of the device is its MAC address.

Views

MST region view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region name.

Examples

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

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

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

revision-level

vlan-mapping modulo

reset stp

Use **reset stp** to clear the spanning tree statistics.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*. If you do not specify this option, this command clears the spanning tree statistics on all ports.

Examples

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

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

Related commands

display stp

revision-level

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

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

Syntax

revision-level *level*

undo revision-level

Default

The MSTP revision level is 0.

Views

MST region view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region level.

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
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

region-name

vlan-mapping modulo

snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send notifications if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.
- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

Enable SNMP notifications for new-root election events.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

stp bpdu-protection

Use **stp bpdu-protection** to enable BPDU guard globally.

Use **undo stp bpdu-protection** to disable BPDU guard globally.

Syntax

stp bpdu-protection

undo stp bpdu-protection

Default

BPDU guard is globally disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable BPDU guard globally.

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

Related commands

stp edged-port

stp bridge-diameter

Use **stp bridge-diameter** to set the network diameter. The switched network diameter refers to the maximum number of devices on the path for an edge device to reach another through the root bridge.

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

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

Default

The network diameter of the switched network is 7.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP switched network diameter, do not specify this option.

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

Usage guidelines

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, and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers are also set to their defaults.

In STP, RSTP, or MSTP mode, each MST region is considered as a device. The configured network diameter of the switched network takes effect only on the CIST (or the common root bridge).

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

Examples

In MSTP mode, set the network diameter of the switched network to 5.

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

In PVST mode, set the network diameter of VLAN 2 in the switched network to 5.

```
<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5
```

Related commands

stp timer forward-delay

stp timer hello

stp timer max-age

stp compliance

Use **stp compliance** to configure the mode a port uses to recognize and send MSTP BPDUs.

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

Syntax

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

undo stp compliance

Default

A port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

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

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

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

Usage guidelines

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

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

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

stp config-digest-snooping

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

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

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

Default

Digest Snooping is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

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

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

Related commands

display stp

stp global config-digest-snooping

stp cost

Use **stp cost** to set the path cost of a port.

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

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

Default

The device automatically calculates the path costs of ports in each spanning tree based on the corresponding standard.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

cost-value: Specifies the path cost of the port, with an effective range that varies by path cost calculation standard that is used.

- When the IEEE 802.1d-1998 standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 65535.
- When the IEEE 802.1t standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000000.
- When the private standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000.

Usage guidelines

Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links. This results in VLAN-based load balancing.

The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, the system calculates the role of the port and initiates a state transition.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, is takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command sets the path cost of a port in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the path cost to 200 for GigabitEthernet 1/0/1 in MSTI 2.

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

In PVST mode, set the path cost to 200 for GigabitEthernet 1/0/1 in VLAN 2.

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

Related commands

display stp

stp pathcost-standard

stp edged-port

Use **stp edged-port** to configure a port as an edge port.

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

Syntax

stp edged-port

undo stp edged-port

Default

All ports are non-edge ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A port directly connecting to a user terminal rather than another device or a shared LAN segment can be configured as an edge port. In case the network topology changes, an edge port does not cause a temporary loop. You can enable the port to transit to the forwarding state rapidly by configuring it as an edge port. As a best practice, configure ports that directly connect to user terminals as edge ports.

Typically, configuration BPDUs from other devices cannot reach an edge port, because the edge port does not connect to any other device. When BPDU guard is disabled on a port configured as an edge port, the port acts as a non-edge port if it receives configuration BPDUs.

On a port, the loop guard feature and the edge port setting are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

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

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

Related commands

stp bpdu-protection

stp loop-protection

stp port bpdu-protection

stp enable

Use **stp enable** to enable the spanning tree feature.

Use **undo stp enable** to disable the spanning tree feature.

Syntax

stp enable

undo stp enable

Default

The spanning tree feature is enabled on all ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

In MSTP mode, disable the spanning tree feature on GigabitEthernet 1/0/1.

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

Related commands

stp global enable

stp mode

stp vlan enable

stp global config-digest-snooping

Use **stp global config-digest-snooping** to enable Digest Snooping globally.

Use **undo stp global config-digest-snooping** to disable Digest Snooping globally.

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

Default

Digest Snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

Examples

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

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

Related commands

display stp

stp config-digest-snooping

stp global enable

Use **stp global enable** to enable the spanning tree feature globally.

Use **undo stp global enable** to disable the spanning tree feature globally.

Syntax

stp global enable

undo stp global enable

Default

The spanning tree feature is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When the spanning tree feature is enabled, the device dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. When the spanning tree feature is disabled, the device stops maintaining the spanning tree status.

Examples

Enable the spanning tree feature globally.

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

Related commands

stp enable

stp mode

stp global mcheck

Use **stp global mcheck** to perform mCheck globally.

Syntax

stp global mcheck

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operate in the original mode.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp global mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

Examples

Perform mCheck globally.

```
<Sysname> system-view
[Sysname] stp global mcheck
```

Related commands

stp mcheck

stp mode

stp ignore-pvid-inconsistency

Use **stp ignore-pvid-inconsistency** to disable inconsistent PVID protection.

Use **undo stp ignore-pvid-inconsistency** to enable inconsistent PVID protection.

Syntax

stp ignore-pvid-inconsistency

undo stp ignore-pvid-inconsistency

Default

Inconsistent PVID protection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when the device is operating in PVST mode.

Disabling inconsistent PVID protection might cause spanning tree calculation errors. To avoid such errors, make sure the following requirements are met:

- Make sure the VLANs on one device do not use the same ID as the PVID of its peer port (except the default VLAN) on another device.
- If the local port or its peer is a hybrid port, do not configure the local and peer ports as untagged members of the same VLAN.
- Disable inconsistent PVID protection on both the local device and the peer device.

Examples

In PVST mode, disable the inconsistent PVID protection feature.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp ignore-pvid-inconsistency
```

stp loop-protection

Use **stp loop-protection** to enable loop guard on a port.

Use **undo stp loop-protection** to disable loop guard on a port.

Syntax

stp loop-protection

undo stp loop-protection

Default

Loop guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable loop guard on GigabitEthernet 1/0/1.

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

Related commands

stp edged-port

stp root-protection

stp max-hops

Use **stp max-hops** to set the maximum number of hops for an MST region.

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

Syntax

stp max-hops *hops*

undo stp max-hops

Default

The maximum number of hops for an MST region is 20.

Views

System view

Predefined user roles

network-admin

Parameters

hops: Specifies the maximum hops in the range of 1 to 40.

Examples

Set the maximum hops of the MST region to 35.

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

Related commands

display stp

stp mcheck

Use **stp mcheck** to perform mCheck on a port.

Syntax

stp mcheck

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operation in the original mode.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, MSTP, or PVST. When Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, MSTP, or PVST with Device C, perform mCheck operations on the ports that connect Device B and Device C.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Perform mCheck on GigabitEthernet 1/0/1.

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

Related commands

stp global mcheck

stp mode

stp mode

Use **stp mode** to configure the spanning tree operating mode.

Use **undo stp mode** to restore the default.

Syntax

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

undo stp mode

Default

A spanning tree device operates in MSTP mode.

Views

System view

Predefined user roles

network-admin

Parameters

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

stp: Configures the spanning tree device to operate in STP mode.

Usage guidelines

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

The PVST mode's compatibility with other modes is as follows:

- **Access port**—The PVST mode is compatible with other modes in any VLAN.
- **Trunk or hybrid port**—The PVST mode is compatible with other modes only in the default VLAN.

Examples

Configure the spanning tree device to operate in STP mode.

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

Related commands

stp enable

stp global enable

stp global mcheck

stp mcheck

stp vlan enable

stp no-agreement-check

Use **stp no-agreement-check** to enable No Agreement Check on a port.

Use **undo stp no-agreement-check** to disable No Agreement Check on a port.

Syntax

stp no-agreement-check

undo stp no-agreement-check

Default

No Agreement Check is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only after you enable it on the root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

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

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

stp pathcost-standard

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

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

Syntax

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

undo stp pathcost-standard

Default

The default standard is **legacy**.

Views

System view

Predefined user roles

network-admin

Parameters

dot1d-1998: Configures the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

dot1t: Configures the device to calculate the default path cost for ports based on IEEE 802.1t.

legacy: Configures the device to calculate the default path cost for ports based on a private standard.

Usage guidelines

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

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
```

Related commands

display stp

stp cost

stp point-to-point

Use **stp point-to-point** to configure the link type of a port.

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

Syntax

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

undo stp point-to-point

Default

The default setting is **auto,** and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

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.

Usage guidelines

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting to let the device automatically detect the port link type.

In MSTP or PVST mode, the **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port takes effect on all MSTIs.

Before you set the link type of a port to point-to-point, make sure the port is connected to a point-to-point link. Otherwise, a temporary loop might occur.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure the link type of GigabitEthernet 1/0/1 as point-to-point.

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

Related commands

display stp

stp port priority

Use **stp port priority** to set the priority of a port. The port priority affects the role of a port in a spanning tree.

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

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

Default

The port priority is 128.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the port priority in the range of 0 to 240 in increments of 16 (as in 0, 16, 32).

Usage guidelines

The smaller the value, the higher the port priority. If all ports on your device use the same priority value, the port priority depends on the port index. The smaller the index, the higher the priority.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command configures the priority of the ports in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the port priority of GigabitEthernet 1/0/1 to 16 in MSTI 2.

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

In PVST mode, set the port priority of GigabitEthernet 1/0/1 to 16 in VLAN 2.

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

```
[Sysname-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

Related commands

display stp

stp port-log

Use **stp port-log** to enable outputting port state transition information.

Use **undo stp port-log** to disable outputting port state transition information.

Syntax

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

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

Default

Outputting port state transition information is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies all MSTIs or VLANs.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Examples

In MSTP mode, enable outputting port state transition information for MSTI 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in MSTI 2 transited to the discarding state and GigabitEthernet 1/0/2 in MSTI 2 transited to the forwarding state.

In PVST mode, enable outputting port state transition information for VLAN 1 through VLAN 4094.

```
<Sysname> system-view
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_DISCARDING: VLAN 2's GigabitEthernet1/0/1 has
been set to discarding state.
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet1/0/2 has
been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in VLAN 2 transited to the discarding state and GigabitEthernet 1/0/2 in VLAN 2 transited to the forwarding state.

stp priority

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

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

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

Default

The device priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the device priority in the range of 0 to 61440 in increments of 4096 (as in 0, 4096, 8192). You can set up to 16 priority values on the device. The smaller the value, the higher the device priority.

Usage guidelines

If you do not specify an MSTI or VLAN, this command configures the priority of the device in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the device priority to 4096 in MSTI 1.

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

In PVST mode, set the device priority to 4096 in VLAN 1.

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

stp pvst-bpdu-protection

Use **stp pvst-bpdu-protection** to enable PVST BPDU guard.

Use **undo stp pvst-bpdu-protection** to disable PVST BPDU guard.

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

Default

PVST BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

PVST BPDU guard enables an MSTP-enabled device to shut down a port if the port receives PVST BPDUs. The shutdown port is brought up after a detection timer expires. To set the detection timer, use the **shutdown-interval** command.

Examples

In MSTP mode, enable PVST BPDU guard.

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

Related commands

shutdown-interval (For more information, see *Fundamentals Command Reference*.)

stp region-configuration

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

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

Syntax

stp region-configuration

undo stp region-configuration

Default

The default settings for an MST region are as follows:

- The MST region name of the device is its MAC address.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

Views

System view

Predefined user roles

network-admin

Usage guidelines

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

Examples

Enter MST region view.

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

stp role-restriction

Use **stp role-restriction** to enable port role restriction.

Use **undo stp role-restriction** to disable port role restriction.

Syntax

stp role-restriction

undo stp role-restriction

Default

Port role restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When port role restriction is enabled on a port, the port cannot become a root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable port role restriction on GigabitEthernet 1/0/1.

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

stp root primary

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

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

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as the root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures the device as the root bridge of the MSTP CIST or of the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as the root bridge of MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

In PVST mode, specify the device as the root bridge of VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

Related commands

stp priority

stp root secondary

stp root secondary

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

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

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a secondary root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The

value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures a secondary root bridge for the MSTP CIST or the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as a secondary root bridge in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root secondary
```

In PVST mode, specify the device as a secondary root bridge in VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root secondary
```

Related commands

stp priority

stp root primary

stp root-protection

Use **stp root-protection** to enable root guard on a port.

Use **undo stp root-protection** to disable root guard on a port.

Syntax

stp root-protection

undo stp root-protection

Default

Root guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature and the root guard feature are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable root guard on GigabitEthernet 1/0/1.

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

Related commands

stp edged-port

stp loop-protection

stp tc-protection

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

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

Syntax

stp tc-protection

undo stp tc-protection

Default

TC-BPDU attack guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With TC-BPDU guard, you can set the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. For TC-BPDUs received that exceed the limit, the device performs a forwarding address entry flush when the interval elapses. This prevents frequent flushing of forwarding address entries.

Examples

Disable TC-BPDU attack guard for the device.

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

Related commands

stp tc-protection threshold

stp tc-protection threshold

Use **stp tc-protection threshold** to set the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.

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

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

Default

By default, the device can perform a maximum of 6 forwarding address entry flushes every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. The value is in the range of 1 to 255.

Examples

Configure the device to perform up to 10 forwarding address entry flushes every 10 seconds.

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

Related commands

stp tc-protection

stp tc-restriction

Use **stp tc-restriction** to enable TC-BPDU transmission restriction.

Use **undo stp tc-restriction** to disable TC-BPDU transmission restriction.

Syntax

stp tc-restriction

undo stp tc-restriction

Default

TC-BPDU transmission restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When TC-BPDU transmission restriction is enabled on a port, the port does not send TC-BPDUs to other ports. It also does not delete MAC address entries.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable TC-BPDU transmission restriction on GigabitEthernet 1/0/1.

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

stp tc-snooping

Use **stp tc-snooping** to enable TC Snooping.

Use **undo stp tc-snooping** to disable TC Snooping.

Syntax

stp tc-snooping

undo stp tc-snooping

Default

TC Snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.

Examples

Globally disable the spanning tree feature and enable TC Snooping.

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

Related commands

stp global enable

stp timer forward-delay

Use **stp timer forward-delay** to set the forward delay timer.

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

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

Default

The forward delay timer is 1500 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP forward delay, do not specify this option.

time: Specifies the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Usage guidelines

The forward delay timer determines the time interval of state transition. To prevent temporary loops, a spanning tree port goes through the learning (intermediate) state before it transits from the discarding state to the forwarding state. To stay synchronized with the remote device, the port has a wait period that is determined by the forward delay timer between transition states.

As a best practice, do not set the forward delay with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

Examples

In MSTP mode, set the forward delay timer to 2000 centiseconds.

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

In PVST mode, set the forward delay timer for VLAN 2 to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer forward-delay 2000
```

Related commands

stp bridge-diameter

stp timer hello

stp timer max-age

stp timer hello

Use **stp timer hello** to set the hello time.

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

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

Default

The hello time is 200 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP hello time, do not specify this option.

time: Specifies the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Usage guidelines

Hello time is the interval at which spanning tree devices send configuration BPDUs to maintain the spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process is triggered.

As a best practice, do not set the hello time with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

Examples

In MSTP mode, set the hello time to 400 centiseconds.

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

In PVST mode, set the hello time for VLAN 2 to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer hello 400
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer max-age

stp timer max-age

Use **stp timer max-age** to set the max age timer.

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

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

Default

The max age is 2000 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP max age, do not specify this option.

time: Specifies the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Usage guidelines

In the CIST of an MSTP network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If the configuration BPDU has expired, a new spanning tree calculation process starts. The max age timer takes effect only on the CIST (or MSTI 0).

As a best practice, do not set the max age timer with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Examples

In MSTP mode, set the max age timer to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

In PVST mode, set the max age timer for VLAN 2 to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer max-age 1000
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer hello

stp timer-factor

Use **stp timer-factor** to configure the timeout period by setting the timeout factor.

Timeout period = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

Syntax

stp timer-factor *factor*

undo stp timer-factor

Default

The timeout factor of the device is set to 3.

Views

System view

Predefined user roles

network-admin

Parameters

factor: Specifies the timeout factor in the range of 1 to 20.

Usage guidelines

In a stable network, each non-root-bridge forwards configuration BPDUs to surrounding devices at the interval of hello time to determine whether any link fails. If a device does not receive a BPDU from the upstream device within nine times of the hello time, it assumes that the upstream device has failed. Then it will start a new spanning tree calculation process.

As a best practice, set the timeout factor to 5, 6, or 7 in the following situations:

- To prevent undesired spanning tree calculations. An upstream device might be too busy to forward configuration BPDUs in time, for example, many Layer 2 interfaces are configured on the upstream device. In this case, the downstream device fails to receive a BPDU within the timeout period and then starts an undesired spanning tree calculation.
- To save network resources on a stable network.

Examples

Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

Related commands

stp timer hello

stp transmit-limit

Use **stp transmit-limit** to set the BPDU transmission rate of a port.

Use **undo stp transmit-limit** to restore the default.

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

Default

The BPDU transmission rate of all ports is 10.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the BPDU transmission rate in the range of 1 to 255.

Usage guidelines

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value.

A larger BPDU transmission rate value requires more system resources. An appropriate BPDU transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. As a best practice, use the default value.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Set the BPDU transmission rate of GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

stp vlan enable

Use **stp vlan enable** to enable the spanning tree feature for VLANs.

Use **undo stp enable** to disable the spanning tree feature for VLANs.

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

Default

The spanning tree feature is enabled in VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

Examples

In PVST mode, globally enable the spanning tree feature and then enable the spanning tree feature for VLAN 2.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp global enable
[Sysname] stp vlan 2 enable
```

Related commands

stp enable

stp global enable

stp mode

vlan-mapping modulo

Use **vlan-mapping modulo** to map VLANs in an MST region to MSTIs according to the specified modulo value and quickly create a VLAN-to-instance mapping table.

Syntax

vlan-mapping modulo *modulo*

Default

All VLANs are mapped to the CIST (MSTI 0).

Views

MST region view

Predefined user roles

network-admin

Parameters

modulo: Specifies the modulo value. The value range for this argument is 1 to 64.

Usage guidelines

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

This command maps each VLAN to the MSTI with ID (VLAN ID – 1) % *modulo* + 1. (VLAN ID – 1) % *modulo* is the modulo operation for (VLAN ID – 1). If the modulo value is 15, then VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, …, VLAN 15 to MSTI 15, VLAN 16 to MSTI 16, and so on.

Examples

Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

revision-level

Contents

LLDP commands 1

display lldp local-information 1
display lldp neighbor-information 5
display lldp statistics 10
display lldp status 13
display lldp tlv-config 15
lldp admin-status 18
lldp check-change-interval 19
lldp enable 20
lldp encapsulation snap 21
lldp fast-count 22
lldp global enable 22
lldp hold-multiplier 23
lldp ignore-pvid-inconsistency 24
lldp management-address 24
lldp management-address-format string 26
lldp max-credit 27
lldp mode 28
lldp notification med-topology-change enable 28
lldp notification remote-change enable 29
lldp source-mac vlan 30
lldp timer fast-interval 31
lldp timer notification-interval 32
lldp timer reinit-delay 33
lldp timer rx-timeout 33
lldp timer tx-interval 34
lldp tlv-enable 35

LLDP commands

The supported interface views depend on the supported interface types, which vary by device model. For more information about the supported interface types, see Ethernet interface configuration in *Interface Configuration Guide*.

display lldp local-information

Use **display lldp local-information** to display local LLDP information.

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global local LLDP information.

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

Usage guidelines

If you do not specify any keywords or arguments, the command displays all local LLDP information, which includes the following:

- The global LLDP information.
- The LLDP information about the LLDP-enabled ports in up state.

Examples

Display all local LLDP information.

```
<Sysname> display lldp local-information
Global LLDP local-information:
 Chassis ID          : 00e0-fc00-5600
 System name         : Sysname
 System description  :
   H3C Comware Platform Software, Software Version 7.1.064, Customer 5424
   H3C WX3510H
   Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported  : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled    : Bridge, Router, Service Bridge

 MED information:
 Device class               : Connectivity device
 MED inventory information of master board:
 HardwareRev                : Ver.A
 FirmwareRev                : 5.12
```

```
 SoftwareRev                : 7.1.064, Customer 5410
 SerialNum                  : 210235A1JNC14B900031
 Manufacturer name          : H3C
 Model name                 : WX3510H
 Asset tracking identifier  : Unknown
LLDP local-information of port 1[GigabitEthernet1/0/1]:
 Port ID type       : Interface name
 Port ID            : GigabitEthernet1/0/1
 Port description   : GigabitEthernet1/0/1 Interface
 LLDP agent nearest-bridge management address:
 Management address type           : IPv4
 Management address                : 192.168.80.60
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 LLDP agent nearest-nontpmr management address:
 Management address type           : IPv4
 Management address                : 192.168.80.61
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 LLDP agent nearest-customer management address:
 Management address type           : IPv4
 Management address                : 192.168.80.62
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 Port VLAN ID(PVID): 1
 Port and protocol VLAN ID(PPVID) : 0
 Port and protocol VLAN supported : No
 Port and protocol VLAN enabled   : No
 VLAN name of VLAN 1: VLAN 0001
 Management VLAN ID  : 5
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID        : 0
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PD
 PSE power supported        : NO
 PSE power enabled          : NO
 PSE pairs control ability  : NO
 Power pairs                : Signal
 Port power classification  : Class 0
 Maximum frame size         : 10000
 Transmit Tw                : 0 us
 Receive Tw                 : 0 us
```

```
Fallback Tw                 : 0 us
Echo Transmit Tw            : 0 us
Echo Receive Tw             : 0 us
PoE PSE power source        : Unknown
Port PSE priority           : Unknown
Port available power value : 0.0 w
```

Table 1 Command output

Field	Description
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **WlanAccessPoint**—The local device can act as a wireless AP. • **Repeater**—Signal repeating is supported. • **Telephone**—The local device can act as a telephone. • **DocsisCableDevice**—The local device can act as a DOCSIS-compliant cable device. • **StationOnly**—The local device can act as a station only. • **Customer Bridge**—The customer bridge feature is supported. • **Service Bridge**—The service bridge feature is supported. • **TPMR**—The TPMR feature is supported. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Enabled capabilities: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **WlanAccessPoint**—The local device is acting as a wireless AP. • **Repeater**—Signal repeating is enabled. • **Telephone**—The local device is acting as a telephone. • **DocsisCableDevice**—The local device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The local device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are enabled.
Device class	MED device class: • **Connectivity device**—Network device. • **Class I**—Normal terminal device. It requires the basic LLDP discovery services. • **Class II**—Media terminal device. It supports media streams, and can also act as a normal terminal device. • **Class III**—Communication terminal device. It supports the IP communication systems of end users, and can also act as a normal terminal device or media terminal device.
MED inventory information of master board	MED inventory information about the MPU.
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.

Field	Description
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
Port ID type	Port ID type: • MAC address. • Interface name.
Port ID	Port ID, the value of which depends on the port ID type.
Management address interface type	Numbering type of the interface identified by the management address.
Management address interface ID	Index 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.
Link aggregation supported	Indicates whether link aggregation is supported on the port.
Link aggregation enabled	Indicates whether link aggregation is enabled on the port.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state of the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
Power priority	• Unknown. • Critical. • High.

Field	Description
	• Low.
PoE PSE power source	PSE power source type: • **Unknown**—Unknown power supply. • **Primary**—Primary power supply. • **Backup**—Backup power supply.
Port PSE priority	PoE power supply priority of PSE ports: • Unknown. • Critical. • High. • Low.
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, in watts.
Transmit Tw	Sleep time of the local client, in μs.
Receive Tw	Sleep time of the peer client expected by the local client, in μs.
Fallback Tw	Candidate sleep time of the peer client expected by the local client, in μs.
Echo Transmit Tw	Sleep time of the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the sleep time of the peer client. • The sleep time of the peer client is 0 μs.
Echo Receive Tw	Sleep time of the local client expected by the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the expected sleep time from the peer client. • The sleep time of the local client expected by the peer client is 0 μs.

display lldp neighbor-information

Use **display lldp neighbor-information** to display the LLDP information received from the neighboring devices.

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the LLDP information that all ports receive from the neighboring devices.

agent: Specifies an agent type. If you do not specify an agent type, the command displays the LLDP information that all LLDP agents receive from the neighboring devices.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

verbose: Displays the detailed LLDP information that the local device receives from the neighboring devices. If you do not specify this keyword, the command displays the brief LLDP information that the local device receives from the neighboring devices.

list: Displays the LLDP information that the local device receives from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information that the local device receives from a neighboring device specified by its system name. The *system-name* argument is a string of 1 to 255 characters. If you do not specify this option, the command displays the LLDP information that the local device receives from all neighboring devices in a list.

Examples

Display detailed LLDP information that the nearest bridge agents on all ports received from the neighboring devices.

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP Neighbor index : 1
 Update time         : 0 days, 0 hours, 1 minutes, 1 seconds
 Chassis type        : MAC address
 Chassis ID          : 000f-0055-0002
 Port ID type        : Interface name
 Port ID             : GigabitEthernet1/0
 Time to live        : 121
 Port description    : GigabitEthernet1/0 Interface
 System name         : Sysname
 System description  :
  H3C Comware Platform Software, Software Version 7.1.064,Release 5534
  H3C WX3024H-L
  Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
 Management address type           : IPv4
 Management address                : 192.168.1.55
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 Port VLAN ID(PVID): 1
 Link aggregation supported : Yes
 Link aggregation enabled   : Yes
 Aggregation port ID        : 52
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PSE
 PSE power supported        : No
```

```
 PSE power enabled          : No
 PSE pairs control ability  : No
 Power pairs                : Signal
 Port power classification  : Class 0
 Power type                 : Type 2 PSE
 Power source               : Primary
 Power priority             : Unknown
 PD requested power value   : 0.0 w
 PSE allocated power value  : 25.5 w
 Maximum frame size         : 1500
```

Display brief LLDP information that all LLDP agents received from all neighboring devices.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 3
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c71f/MAC address
 Capabilities        : Bridge, Router, Customer Bridge

 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None

CDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 4
 Chassis ID          : SEP00260B5C0548
 Port ID             : Port 1

 CDP neighbor index  : 5
 Chassis ID          : 0011-2233-4400
 Port ID             : GigabitEthernet1/0/4

LLDP neighbor-information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-nontpmr:
 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None
```

Display brief LLDP information that all LLDP agents received from the neighboring devices in a list.

```
<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
System Name          Local Interface   Chassis ID       Port ID
System1              GE1/0/2           000f-e25d-ee91   GigabitEthernet1/0/2
```

Table 2 Command output

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1.
Update time	Time when LLDP information about a neighboring device was last updated.
LLDP mac type	Type of the neighbor MAC address: • Nearest bridge. • Nearest customer bridge. • Nearest non-TPMR bridge.
Chassis type	Chassis ID type: • **Chassis component**. • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Locally assigned**—Locally-defined chassis type other than those listed above.
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 ID type of the neighboring device.
Port ID type	Port ID type: • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Agent circuit ID**. • **Locally assigned**—Locally-defined port ID type other than those listed above.
Port ID	Value of the type of the port ID.
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: • **Repeater**—Signal repeating is supported. • **Bridge**—Switching is supported. • **WlanAccessPoint**—The neighboring device can act as a wireless AP. • **Router**—Routing is supported. • **Telephone**—The neighboring device can act as a telephone. • **DocsisCableDevice**—The neighboring device can act as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device can act as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Capabilities enabled on the neighboring device:

Field	Description
	• **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **WlanAccessPoint**—The neighboring device is acting as a wireless AP. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
Management address OID	Management address object ID.
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
Power type	Power supply type: • Type 1 PD. • Type 2 PD. • Type 1 PSE. • Type 2 PSE.
Power source	Power source: • When the power supply type is PSE, options are: ○ **Unknown**—Unknown power supply. ○ **Primary**—Primary power supply.

Field	Description
	○ **Backup**—Backup power supply. ○ **Reserved**. • When the power supply type is PD, options are:: ○ **Unknown**—Unknown power supply. ○ **PSE**—PSE power supply. ○ **Local**—Local power supply. ○ **PSE and local**—PSE and local power supplies.
Power priority	• Unknown. • Critical. • High. • Low.
PD requested power value	2-pair single-signature PD requested power in watts.
PSE allocated power value	2-pair single-signature PSE allocated power in watts.
TLV type	Unknown basic TLV type.
TLV information	Information contained in the unknown basic TLV type.
Unknown organizationally-defined TLV	Unknown organizationally specific TLV.
TLV OUI	OUI of the unknown organizationally specific TLV.
TLV subtype	Unknown organizationally specific TLV subtype.
Index	Unknown organization index.
Capabilities	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **WlanAccessPoint**—The neighboring device is acting as a wireless AP. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Other**—Features other than those listed above are supported. • **None**—The neighboring device does not advertise this TLV.
Local Interface	Local port that receives the LLDP information.
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	Chassis ID flag: • An asterisk (*) indicates the nearest non-TPMR bridge neighbor. • A pound sign (#) indicates the nearest customer bridge neighbor.

display lldp statistics

Use **`display lldp statistics`** to display the global LLDP statistics or the LLDP statistics of a port.

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global LLDP statistics.

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

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

If you do not specify any keywords or arguments, the command displays the global LLDP statistics and the LLDP statistics of all ports.

Examples

Display the global LLDP statistics and the LLDP statistics of all ports.

```
<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 1
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

```
LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
…
```

Display the LLDP statistics for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> display lldp statistics interface gigabitethernet 1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Table 3 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time when the neighbor information was last updated.

Field	Description
The number of LLDP neighbor information inserted	Number of times neighbor information was added.
The number of LLDP neighbor information deleted	Number of times neighbor information was removed.
The number of LLDP neighbor information dropped	Number of times neighbor information was dropped due to lack of available memory space.

display lldp status

Use **display lldp status** to display LLDP status.

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the global LLDP status and the LLDP status of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the status information for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the global LLDP status and the LLDP status of each port.

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 5s
Fast start times               : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
```

```
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5
...
```

Table 4 Command output

Field	Description
Bridge mode of LLDP	LLDP bridge mode: service-bridge or customer-bridge.
Global status of LLDP	Indicates whether LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDP frame transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP reinitialization delay.

Field	Description
Transmit max credit	Token bucket size for sending LLDP frames.
Trap interval	Trap transmission interval.
Fast start times	Number of LLDP frames sent each time fast LLDP frame transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether LLDP is enabled on the port.
Admin status	LLDP operating mode of the port: • **TX_RX**—The port can send and receive LLDP frames. • **Rx_Only**—The port can only receive LLDP frames. • **Tx_Only**—The port can only send LLDP frames. • **Disable**—The port cannot send or receive LLDP frames.
Trap Flag	Indicates whether trapping is enabled.
Polling interval	LLDP polling interval, which is 0 when LLDP polling is disabled.
Number of neighbors	Number of LLDP neighbors connecting to the port.
Number of MED neighbors	Number of MED neighbors connecting to the port.
Number of CDP neighbors	Number of CDP neighbors connecting to the port.
Number of sent optional TLV	Number of optional TLVs contained in an LLDP frame sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in a received LLDP frame.

display lldp tlv-config

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the types of advertisable optional TLVs of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the types of advertisable optional LLDP TLVs for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the types of advertisable optional LLDP TLVs of GigabitEthernet 1/0/1.

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
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
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               YES       YES
 Congestion notification TLV      NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       YES
 Power via MDI TLV                YES       YES
 Maximum Frame Size TLV           YES       YES
 Energy-Efficient Ethernet TLV    NO        NO
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
LLDP agent nearest-nontpmr:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       NO
 System Name TLV                  YES       NO
 System Description TLV           YES       NO
 System Capabilities TLV          YES       NO
 Management Address TLV           YES       NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       NO
 Port And Protocol VLAN ID TLV    YES       NO
 VLAN Name TLV                    YES       NO
 DCBX TLV                         NO        NO
 EVB TLV                          YES       YES
 Link Aggregation TLV             YES       NO
```

```
 Management VID TLV              NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                  YES       NO
 Power via MDI TLV               YES       NO
 Maximum Frame Size TLV          YES       NO
 Energy-Efficient Ethernet TLV   NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                YES        NO
 Network Policy TLV              YES        NO
 Location Identification TLV     NO         NO
 Extended Power via MDI TLV      YES        NO
 Inventory TLV                   YES        NO

LLDP agent nearest-customer:
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
 DCBX TLV                        NO        NO
 EVB TLV                         NO        NO
 Link Aggregation TLV            YES       NO
 Management VID TLV              YES       YES
IEEE 802.3 extend TLV:
 MAC-Physic TLV                  YES       NO
 Power via MDI TLV               YES       NO
 Maximum Frame Size TLV          YES       NO
 Energy-Efficient Ethernet TLV   NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                YES        YES
 Network Policy TLV              YES        YES
 Location Identification TLV     NO         NO
 Extended Power via MDI TLV      YES        NO
 Inventory TLV                   YES        YES
```

Table 5 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether the type of TLV is sent through a port.
DEFAULT	Indicates whether the type of TLV is sent through a port by default.

Field	Description
Basic optional TLV	Basic optional TLVs: • Port Description TLV. • System Name TLV. • System Description TLV. • System Capabilities TLV. • Management Address TLV. • Congestion notification TLV. Congestion notification TLVs are not supported in the current software version.
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: • Port VLAN ID TLV. • Port and protocol VLAN ID TLV. • VLAN name TLV. • DCBX TLV. DCBX TLVs are not supported in the current software version. • EVB TLV. EVB TLVs are not supported in the current software version. • Management VID TLV.
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs: • MAC-Physic TLV. • Power via MDI TLV. • Link aggregation TLV. • Maximum frame size TLV.
LLDP-MED extend TLV	LLDP-MED TLVs: • Capabilities TLV. • Network Policy TLV. • Extended Power-via-MDI TLV. • Location Identification TLV. • Inventory TLV.
Inventory TLV	Inventory TLVs: • Hardware Revision TLV. • Firmware Revision TLV. • Software Revision TLV. • Serial Number TLV. • Manufacturer Name TLV. • Model name TLV. • Asset ID TLV.
Energy-Efficient Ethernet TLV	Indicates the Energy-Efficient Ethernet TLV.

lldp admin-status

Use **lldp admin-status** to set the LLDP operating mode.

Use **undo lldp admin-status** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status**

Default

The nearest bridge agent operates in **TxRx** mode, and the nearest customer bridge agent and nearest non-TPMR bridge agent operate in **Disable** mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the operating mode for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

disable: Specifies the **Disable** mode. A port in this mode cannot send or receive LLDP frames.

rx: Specifies the **Rx** mode. A port in this mode can only receive LLDP frames.

tx: Specifies the **Tx** mode. A port in this mode can only send LLDP frames.

txrx: Specifies the **TxRx** mode. A port in this mode can send and receive LLDP frames.

Examples

Set the LLDP operating mode to **Rx** for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

lldp check-change-interval

Use **lldp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo lldp check-change-interval** to disable LLDP polling.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval**

Default

LLDP polling is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP polling and sets the polling interval for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

interval: Sets the LLDP polling interval in the range of 1 to 30 seconds.

Examples

Enable LLDP polling and set the polling interval to 30 seconds for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

lldp enable

Use **lldp enable** to enable LLDP on a port.

Use **undo lldp enable** to disable LLDP on a port.

Syntax

lldp enable

undo lldp enable

Default

LLDP is enabled on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

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

Examples

Disable LLDP on GigabitEthernet 1/0/1.

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

Related commands

lldp global enable

lldp encapsulation snap

Use **lldp encapsulation snap** to set the encapsulation format for LLDP frames to SNAP.

Use **undo lldp encapsulation** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation**

Default

The encapsulation format for LLDP frames is Ethernet II.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the LLDP frame encapsulation format for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

Examples

Set the encapsulation format for LLDP frames to SNAP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

lldp fast-count

Use **lldp fast-count** to set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Use **undo lldp fast-count** to restore the default.

Syntax

lldp fast-count *count*

undo lldp fast-count

Default

Four LLDP frames are sent each time fast LLDP frame transmission is triggered.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of LLDP frames sent each time fast LLDP frame transmission is triggered. The value range is 1 to 8.

Examples

Configure the device to send five LLDP frames each time fast LLDP frame transmission is triggered.

```
<Sysname> system-view
[Sysname] lldp fast-count 5
```

lldp global enable

Use **lldp global enable** to enable LLDP globally.

Use **undo lldp global enable** to disable LLDP globally.

Syntax

lldp global enable

undo lldp global enable

Default

LLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

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

Examples

Disable LLDP globally.

```
<Sysname> system-view
[Sysname] undo lldp global enable
```

Related commands

lldp enable

lldp hold-multiplier

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier to** restore the default.

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

Default

The TTL multiplier is 4.

Views

System view

Predefined user roles

network-admin

Parameters

value: Sets the TTL multiplier in the range of 2 to 10.

Usage guidelines

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can set the TTL of locally sent LLDP frames. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds.

Examples

Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

Related commands

lldp timer tx-interval

lldp ignore-pvid-inconsistency

Use **lldp ignore-pvid-inconsistency** to disable LLDP PVID inconsistency check.

Use **undo lldp ignore-pvid-inconsistency** to enable LLDP PVID inconsistency check.

Syntax

lldp ignore-pvid-inconsistency

undo lldp ignore-pvid-inconsistency

Default

LLDP PVID inconsistency check is enabled.

Views

System view

Default command level

network-admin

Usage guidelines

By default, when the system receives an LLDP packet, it compares the PVID value contained in packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

Examples

Disable LLDP PVID inconsistency check.

```
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

lldp management-address

Use **lldp management-address** to enable the device to generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Use **undo lldp management-address** to restore the default.

Syntax

lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

undo lldp management-address { **arp-learning** | **nd-learning** }

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204	EWP-MAK204	Yes

Hardware series	Model	Product code	Command compatibility
	MAK206	EWP-MAK206	
WX3000H series	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L • WX3010H-X • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Default

The device does not generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Views

Layer 3 Ethernet interface view

Default command level

network-admin

Parameters

arp-learning: Generates an ARP entry if the received management address TLV contains an IPv4 address.

nd-learning: Generates an ND entry if the received management address TLV contains an IPv6 address.

vlan *vlan-id*: Specifies the ID of a Layer 3 Ethernet subinterface in the range of 1 to 4094. The subinterface will be recorded as the output interface in the ARP or ND entry. If the Layer 3 Ethernet subinterface does not exist or if this option is not specified, the Layer 3 Ethernet interface is recorded as the output interface.

Usage guidelines

You can enable the device to generate both ARP entries and ND entries.

Examples

Configure GigabitEthernet 1/0/1 to generate an ARP entry after receiving an LLDP frame carrying an IPv4 management address TLV.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address arp-learning
```

Related commands

lldp source-mac vlan

lldp management-address-format string

Use **lldp management-address-format string** to set the encoding format of the management address to string.

Use **undo lldp management-address-format** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view/management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **management-address-format string**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **management-address-format**

Default

The encoding format of the management address is numeric.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the encoding format of the management address for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP neighbors must use the same encoding format for the management address. If a neighbor encodes its management address in string format, set the encoding format of the management address to **string** on the connecting port. This guarantees normal communication with the neighbor.

Examples

Set the encoding format of the management address to string for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format
string
```

lldp max-credit

Use **lldp max-credit** to set the token bucket size for sending LLDP frames.

Use **undo lldp max-credit** to restore the default.

Syntax

lldp max-credit *credit-value*

undo lldp max-credit

Default

The token bucket size for sending LLDP frames is 5.

Views

System view

Predefined user roles

network-admin

Parameters

credit-value: Specifies the token bucket size for sending LLDP frames, in the range of 1 to 100.

Examples

Set the token bucket size for sending LLDP frames to 10.

```
<Sysname> system-view
[Sysname] lldp max-credit 10
```

lldp mode

Use **lldp mode** to configure LLDP to operate in service bridge mode.

Use **undo lldp mode** to restore the default.

Syntax

lldp mode service-bridge

undo lldp mode

Default

LLDP operates in customer bridge mode.

Views

System view

Predefined user roles

network-admin

Parameters

service-bridge: Specifies the service bridge mode.

Usage guidelines

The LLDP agent types supported by LLDP depend on the LLDP bridge mode:

- **Service bridge mode**—LLDP supports nearest bridge agents and nearest non-TPMR bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.
- **Customer bridge mode**—LLDP supports nearest bridge agents, nearest non-TPMR bridge agents, and nearest customer bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.

The bridge mode configuration takes effect only when LLDP is enabled globally. If LLDP is disabled globally, LLDP can only operate in customer bridge mode.

Examples

Configure LLDP to operate in service bridge mode.

```
<Sysname> system-view
[Sysname] lldp mode service-bridge
```

Related commands

lldp global enable

lldp notification med-topology-change enable

Use **lldp notification med-topology-change enable** to enable LLDP-MED trapping.

Use **undo lldp notification med-topology-change enable** to disable LLDP-MED trapping.

Syntax

lldp notification med-topology-change enable

undo lldp notification med-topology-change enable

Default

LLDP-MED trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Examples

Enable LLDP-MED trapping on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable
```

lldp notification remote-change enable

Use **lldp notification remote-change enable** to enable LLDP trapping.

Use **undo lldp notification remote-change enable** to disable LLDP trapping.

Syntax

In Layer 2/Layer 3 Ethernet interface view/management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

Default

LLDP trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP trapping for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Enable LLDP trapping for the nearest customer bridge agent on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change
enable
```

lldp source-mac vlan

Use **lldp source-mac vlan** to set the source MAC address of LLDP frames to the MAC address of a Layer 3 Ethernet subinterface.

Use **undo lldp source-mac vlan** to restore the default.

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L • WX3010H-X • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller	LSUM1WCME0	LSUM1WCME0	No

Hardware series	Model	Product code	Command compatibility
modules	EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Syntax

lldp source-mac vlan *vlan-id*

undo lldp source-mac vlan

Default

The source MAC address of LLDP frames is the MAC address of the egress interface.

Views

Layer 3 Ethernet interface view

Default command level

network-admin

Parameters

vlan *vlan-id*: Specifies the ID of a Layer 3 Ethernet subinterface, in the range of 1 to 4094. If the Layer 3 Ethernet subinterface does not exist, the MAC address of the Layer 3 Ethernet interface is used as the source MAC address of LLDP frames.

Examples

Set the source MAC address of LLDP frames to the MAC address of a Layer 3 Ethernet subinterface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp source-mac vlan 4094
```

Related commands

lldp management-address arp-learning

lldp timer fast-interval

Use **lldp timer fast-interval** to set an interval for fast LLDP frame transmission.

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

Syntax

lldp timer fast-interval *interval*

undo lldp timer fast-interval

Default

The interval for fast LLDP frame transmission is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets an interval for fast LLDP frame transmission, in the range of 1 to 3600 seconds.

Examples

Set the interval for fast LLDP frame transmission to 2 seconds.

```
<Sysname> system-view
[Sysname] lldp timer fast-interval 2
```

lldp timer notification-interval

Use **lldp timer notification-interval** to set the LLDP trap and LLDP-MED trap transmission interval.

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

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

Default

The LLDP trap and LLDP-MED trap transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP trap and LLDP-MED trap transmission interval in the range of 5 to 3600 seconds.

Examples

Set both the LLDP trap and LLDP-MED trap transmission interval to 8 seconds.

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

lldp timer reinit-delay

Use **lldp timer reinit-delay** to set the LLDP reinitialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

Default

The LLDP reinitialization delay is 2 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay: Sets the LLDP reinitialization delay in the range of 1 to 10 seconds.

Examples

Set the LLDP reinitialization delay to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer rx-timeout

Use **lldp timer rx-timeout** to set the timeout for receiving LLDP frames and enable the device to report no LLDP neighbor events.

Use **undo lldp timer rx-timeout** to restore the default.

Syntax

lldp timer rx-timeout *timeout*

undo lldp timer rx-timeout

Default

No timeout is set for receiving LLDP frames, and the device does not report no LLDP neighbor events.

Views

System view

Predefined user roles

network-admin

Parameters

timeout: Sets the timeout for receiving LLDP frames, in the range of 30 to 32768 seconds.

Usage guidelines

This command can detect only directly connected LLDP neighbors.

When you use this command, make sure the following requirements are met:

- LLDP is enabled.
- Interfaces are physically up.
- Nearest bridge agents operate in **Rx** or **TxRx** mode.

After this command is executed, the device restarts the timeout timer for receiving LLDP frames on an interface in one of the following situations:

- When LLDP is enabled, the interface state changes from down to up.
- When the interface is physically up, LLDP is enabled.
- When LLDP is enabled and the interface is physically up, the mode of nearest bridge agents is changed from disabled to **Rx** or **TxRx**.

If an interface has not received any LLDP frames when the timeout timer expires, the device reports a no LLDP neighbor event to the NETCONF module.

To avoid misdetection, make sure the timeout for receiving LLDP frames is greater than the LLDP frame transmission interval.

Examples

Set the timeout for receiving LLDP frames to 30 seconds.

```
<Sysname> system-view
[Sysname] lldp timer rx-timeout 30
```

Related commands

lldp timer tx-interval

lldp timer tx-interval

Use **lldp timer tx-interval** to set the LLDP frame transmission interval.

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

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

Default

The LLDP frame transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP frame transmission interval in the range of 5 to 32768 seconds.

Examples

Set the LLDP frame transmission interval to 20 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

lldp tlv-enable

Use **lldp tlv-enable** to configure the types of advertisable TLVs on a port.

Use **undo lldp tlv-enable** to disable the advertising of the specified types of TLVs on a port.

Syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** |

system-capability | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

Default

On Layer 2 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except the following types:
  - Location identification TLVs.
  - Port and protocol VLAN ID TLVs.
  - VLAN name TLVs.
  - Management VLAN ID TLVs.
- Nearest non-TPMR bridge agents do not advertise any TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

On Layer 3 Ethernet interfaces or management Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except network policy TLVs. Among all the 802.1 organizationally specific TLVs, only the link aggregation TLV is supported.
- Nearest non-TPMR bridge agents do not advertise TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On Layer 2 aggregate interfaces:

- Nearest non-TPMR bridge agents do not advertise any TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs. Among the IEEE 802.1 organizationally specific TLVs, only port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs are supported.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command configures the types of advertisable TLVs for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

all: Advertises all TLVs of the specified type. This keyword enables the interface to advertise following TLVs:

- All basic LLDP TLVs if the **all** keyword is specified for **basic-tlv**.
- All IEEE 802.1 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot1-tlv**.
- All IEEE 802.3 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot3-tlv**.
- All LLDP-MED TLVs except location identification TLVs if the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP TLVs.

management-address-tlv [**ipv6**] [*ip-address* | **interface loopback** *interface-number*]: Advertises management address TLVs. The **ipv6** keyword indicates that the management address to be advertised is in IPv6 format. The *ip-address* argument specifies the management address to be advertised. The **interface loopback** *interface-number* option specifies the management address as the IP address of a loopback interface specified by its number. By default, the following rules apply:

- When you execute the **lldp tlv-enable** command:
  - For a Layer 2 Ethernet or aggregate interface, the IPv4 or IPv6 address of the VLAN interface that meets the following requirements will be advertised as the management address:
    - In up state.
    - The corresponding VLAN ID is the lowest among the VLANs permitted on the interface.

    If you specify the **ipv6** keyword, the IPv6 address of the VLAN interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the VLAN interface will be advertised.

    If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 or IPv6 address or all VLAN interfaces are down, the MAC address of the interface will be advertised.
  - For a Layer 3 Ethernet interface, the IPv4 or IPv6 address of the interface will be advertised when the following conditions exist:
    - The *ip-address* argument is not configured.
    - The specified loopback interface does not have an IPv4 or IPv6 address, or the specified loopback interface does not exist.

    If you specify the **ipv6** keyword, the IPv6 address of the interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the interface will be advertised.

    If the interface does not have an IPv4 or IPv6 address, the MAC address of the interface will be advertised.
  - For a management Ethernet interface, the IPv4 or IPv6 address of the interface will be advertised when the *ip-address* argument is not configured.

    If you specify the **ipv6** keyword, the IPv6 address of the interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the interface will be advertised.

If the interface does not have an IPv4 or IPv6 address, the MAC address of the interface will be advertised.

- When you execute the **undo lldp tlv-enable** command:
  - For a Layer 2/Layer 3 Ethernet interface, management Ethernet interface, or Layer 2 aggregate interface:
    - If you do not specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface does not advertise any management address TLVs.
    - If you specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface advertises the default management address TLVs.

port-description: Advertises port description TLVs.

system-capability: Advertises system capabilities TLVs.

system-description: Advertises system description TLVs.

system-name: Advertises system name TLVs.

dot1-tlv: Advertises IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Advertises port VLAN ID TLVs.

protocol-vlan-id [*vlan-id*]: Advertises port and protocol VLAN ID TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port.

vlan-name [*vlan-id*]: Advertises VLAN name TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised.

management-vid [*mvlan-id*]: Advertises management VLAN ID TLVs. The m*vlan-id* argument specifies a management VLAN ID in the TLVs to be advertised. The management VLAN ID is in the range of 1 to 4094. If you do not specify this option, the value 0 is advertised, which means that the LLDP agent is not configured with a management VLAN ID.

link-aggregation: Advertises link aggregation TLVs.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power in MDI TLVs and power stateful control TLVs.

med-tlv: Advertises LLDP-MED TLVs.

capability: Advertises LLDP-MED capabilities TLVs.

inventory: Advertises the following TLVs: hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

location-id: Advertises location identification TLVs.

civic-address: Inserts the typical address information about the network device in location identification TLVs .

device-type: Sets a device type value in the range of 0 to 2:

- Value 0 specifies a DHCP server.
- Value 1 specifies a network device.
- Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code defined in ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information. *ca-type* represents the address information type in the range of 0 to 255. *ca-value* represents address information, a string of 1 to 250 characters. &<1-10> indicates that you can specify up to 10 *ca-type ca-value* pairs.

elin-address: Inserts telephone numbers for emergencies in location identification TLVs.

tel-number: Sets the telephone number for emergencies, a string of 10 to 25 characters.

network-policy [*vlan-id*]: Advertises network policy TLVs. The *vlan-id* argument specifies the voice VLAN ID to be advertised, in the range of 1 to 4094.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Usage guidelines

Nearest bridge agents are not supported on aggregate interfaces.

You can enable the device to advertise multiple types of TLVs by using this command without the **all** keyword specified.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised whether or not they are advertisable. If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised regardless of whether or not they are advertisable.

The port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs in IEEE 802.1 organizationally specific LLDP TLVs can be configured only for nearest bridge agents. The configuration can be inherited by nearest customer bridge agents and nearest non-TPMR bridge agents.

Examples

Enable the nearest customer bridge agents on GigabitEthernet 1/0/1 to advertise link aggregation TLVs of the IEEE 802.1 organizationally specific TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

Contents

Layer 2 forwarding commands 1
Normal Layer 2 forwarding commands 1
display mac-forwarding statistics 1
reset mac-forwarding statistics 3
Fast Layer 2 forwarding commands 3
display mac-forwarding cache ip 3
display mac-forwarding cache ip fragment 4
display mac-forwarding cache ipv6 6

Layer 2 forwarding commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

Normal Layer 2 forwarding commands

display mac-forwarding statistics

Use **display mac-forwarding statistics** to display Layer 2 forwarding statistics.

Syntax

display mac-forwarding statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays Layer 2 forwarding statistics on all interfaces.

Examples

Display Layer 2 forwarding statistics on all interfaces.

```
<Sysname> display mac-forwarding statistics
Input:
   Sum:               888        Unknown Unicast:   0
   Broadcast:         0          Multicast:         0
   Filtered:          0          STP discarded:     0
   Service dropped:   0          Source dropped:    0
   Unknown dropped: 0          Learning dropped:  0
   Blackhole dropped: 0          Suppress dropped:  0
   Source MAC dropped:0
Deliver:
   Sum:               111        L2 protocol:       11
   Local MAC address: 100
Output:
   Sum:               666        Filtered:          0
   Blackhole dropped: 0          STP discarded:     0
```

```
   Service dropped:   0          Dest MAC dropped:  0
```

Display Layer 2 forwarding statistics on GigabitEthernet 1/0/1.

```
<Sysname> display mac-forwarding statistics interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Input frames: 100    Output frames:100
Filtered:     0
```

Table 1 Command output

Field	Description
Input	Inbound Ethernet frame statistics. • **Sum**—Total number of received Ethernet frames. • **Filtered**—Number of Ethernet frames filtered out by 802.1Q VLAN inbound filtering rules. • **STP discarded**—Number of inbound Ethernet frames dropped on the ports blocked by STP. • **Service dropped**—Number of Ethernet frames dropped by inbound service features. • **Source dropped**—Number of Ethernet frames dropped because their source MAC addresses are all-zeros, multicast, or broadcast MAC addresses. • **Unknown dropped**—Number of Ethernet frames dropped because the device is disabled from forwarding frames with unknown source MAC addresses. • **Learning dropped**—Number of Ethernet frames dropped because the device is disabled from forwarding unknown frames after the number of learned MAC addresses reaches the upper limit. • **Suppress dropped**—Number of Ethernet frames dropped by storm suppression. • **Broadcast**—Number of received broadcast Ethernet frames. • **Multicast**—Number of received multicast Ethernet frames. • **Unknown unicast**—Number of received unknown unicast Ethernet frames. • **Blackhole dropped**—Number of Ethernet frames dropped because they are sourced from blackhole MAC addresses. • **Source MAC dropped**—Number of Ethernet frames dropped by features based on the source MAC addresses.
Deliver	Statistics of Ethernet frames delivered to the CPU. • **Sum**—Total number of Ethernet frames delivered to the CPU. • **L2 protocol**—Number of Layer 2 protocol Ethernet frames delivered to the CPU. • **Local MAC address**—Number of Ethernet frames that use the MAC addresses of local Layer 3 VLAN interfaces as the destination MAC addresses.
Output	Outbound Ethernet frame statistics. • **Sum**—Total number of sent Ethernet frames. • **Filtered**—Number of Ethernet frames filtered out by 802.1Q VLAN outbound filtering rules. • **Blackhole dropped**—Number of Ethernet frames dropped because they are destined for blackhole MAC addresses. • **STP discarded**—Number of outbound Ethernet frames dropped on the ports blocked by STP. • **Service dropped**—Number of Ethernet frames dropped by outbound service features. • **Dest MAC dropped**—Number of Ethernet frames dropped by features

Field	Description
	based on the destination MAC addresses.
GigabitEthernet1/0/1	Layer 2 forwarding statistics on GigabitEthernet 1/0/1: • **Input frames**—Number of Ethernet frames received on the interface. • **Output frames**—Number of Ethernet frames sent out of the interface. • **Filtered**—Number of Ethernet frames filtered out because they are from other VLANs.

reset mac-forwarding statistics

Use **reset mac-forwarding statistics** to clear Layer 2 forwarding statistics.

Syntax

reset mac-forwarding statistics

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Clear Layer 2 forwarding statistics.

```
<Sysname> reset mac-forwarding statistics
```

Fast Layer 2 forwarding commands

display mac-forwarding cache ip

Use **display mac-forwarding cache ip** to display IPv4 fast forwarding entries.

Syntax

In standalone mode:

display mac-forwarding cache ip [*ip-address*]

In IRF mode:

display mac-forwarding cache ip [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays all IPv4 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for all member devices. (In IRF mode.)

Examples

Display all IPv4 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ip
Total number of mac-forwarding entries: 2
SIP            SPort DIP            DPort Pro Input_If    Output_If   VLAN
1.1.1.2        99    1.1.1.1        2048  1   GE1/0/1     GE1/0/2     2
1.1.1.1        98    1.1.1.2        2012  1   GE1/0/2     GE1/0/1     2
```

Table 2 Command output

Field	Description
Total number of mac-forwarding entries	Total number of IPv4 fast forwarding entries.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
Output_If	Output interface type and number. If no output interface is involved in fast forwarding, this field displays **N/A**. If no output interface is available, this field displays a hyphen (-).
VLAN	VLAN ID.

display mac-forwarding cache ip fragment

Use **display mac-forwarding cache ip fragment** to display IPv4 fast forwarding entries for fragments.

Syntax

In standalone mode:

display mac-forwarding cache ip fragment [*ip-address*]

In IRF mode:

display mac-forwarding cache ip fragment [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays IPv4 fast forwarding entries for all fragments.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for fragments on all member devices. (In IRF mode.)

Examples

Display IPv4 fast forwarding entries for all fragments.

```
<Sysname> display mac-forwarding cache ip fragment
Total number of fragment mac-forwarding entries: 2
SIP             SPort DIP             DPort Pro Input_If    ID     VLAN
1.1.1.1         117   1.1.1.2         0     1   GE1/0/1     2828   1
1.1.1.2         110   1.1.1.1         67    17  GE1/0/2     2322   1
```

Table 3 Command output

Field	Description
Total number of fragment mac-forwarding entries	Total number of IPv4 fast forwarding entries for fragments.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
ID	Fragment ID.
VLAN	VLAN ID.

display mac-forwarding cache ipv6

Use **display mac-forwarding cache ipv6** to display IPv6 fast forwarding entries.

Syntax

In standalone mode:

display mac-forwarding cache ipv6 [*ipv6-address*]

In IRF mode:

display mac-forwarding cache ipv6 [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for all member devices. (In IRF mode.)

Examples

Display all IPv6 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ipv6
Total number of IPv6 mac-forwarding items: 1
Src IP: 2002::1                                    Src port: 129
Dst IP: 2001::1                                    Dst port: 65535
VLAN ID: 2
Protocol: 2
Input interface: GE1/0/2
Output interface: GE1/0/1
```

Table 4 Command output

Field	Description
Total number of IPv6 mac-forwarding items	Total number of IPv6 fast forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.

Field	Description
Input interface	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
Output interface	Output interface type and number. If no output interface is involved in fast forwarding, this field displays **N/A**. If no output interface is available, this field displays a hyphen (-).

Contents

VLAN termination commands 1

second-dot1q 2
vlan-termination broadcast enable 3
vlan-termination broadcast ra 4
vlan-type dot1q default 5
vlan-type dot1q untagged 6
vlan-type dot1q vid 6
vlan-type dot1q vid second-dot1q 7

VLAN termination commands

The following compatibility matrixes show the support of hardware platforms for VLAN termination:

Hardware series	Model	Product code	VLAN termination compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3010H-X-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	VLAN termination compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

second-dot1q

Use **second-dot1q** to enable QinQ termination on an interface, and specify the Layer 2 VLAN IDs of the VLAN-tagged packets that can be terminated by the interface.

Use **undo second-dot1q** to disable QinQ termination on an interface.

Syntax

second-dot1q { *vlan-id-list* | **any** }

undo second-dot1q { *vlan-id-list* | **any** }

Default

QinQ termination is disabled on an interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 Layer 2 VLAN ID items. Each item specifies a Layer 2 VLAN ID or a range of Layer 2 VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

any: Specifies all values between 1 and 4094.

Usage guidelines

When you execute this command, the Layer 1 VLAN ID of VLAN-tagged packets that can be terminated by the interface is the interface number. This Layer 1 VLAN ID is not configurable.

Examples

Configure VLAN-interface 10 to terminate VLAN-tagged packets with Layer 2 VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] second-dot1q 10 to 20
[Sysname-Vlan-interface10] quit
```

Configure VLAN-interface 12 to terminate VLAN-tagged packets with Layer 2 VLAN ID 100.

```
[Sysname] interface vlan-interface 12
```

```
[Sysname-Vlan-interface12] second-dot1q 100
[Sysname-Vlan-interface12] quit
```

Configure VLAN-interface 100 to terminate VLAN-tagged packets with any Layer 2 VLAN IDs.

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] second-dot1q any
```

The following table describes the configuration results:

VLAN interface	Layer 1 VLAN ID of VLAN-tagged packets that the VLAN interface can terminate	Layer 2 VLAN IDs of VLAN-tagged packets that the VLAN interface can terminate
VLAN-interface 10	10	10–20
VLAN-interface 12	12	100
VLAN-interface 100	100	1–4094

vlan-termination broadcast enable

Use **vlan-termination broadcast enable** to enable an interface to transmit broadcasts and multicasts.

Use **undo vlan-termination broadcast enable** to disable an interface from transmitting broadcasts and multicasts.

Syntax

vlan-termination broadcast enable

undo vlan-termination broadcast enable

Default

An ambiguous Dot1q or QinQ termination-enabled interface drops broadcast and multicast packets.

Views

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

IMPORTANT:

This command affects system performance. If system performance is seriously affected by this command, execute the **undo** form of this command to remove the command configuration.

.To transmit a broadcast or multicast packet, the interface starts a traversal over the VLAN IDs specified for ambiguous termination. It copies the packet and tags each copy with a VLAN ID, until all VLAN IDs in the specified range are traversed. For example, when ambiguous QinQ termination is configured, both layers of VLAN ID ranges are traversed.

Use this command when ambiguous Dot1q or QinQ termination is enabled on an interface.

Examples

Configure GigabitEthernet 1/0/1.10 to tag a multicast or broadcast packet with each VLAN tag in the range of 10 to 20.

Enable Dot1q termination on GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 10 to 20
```

Enable GigabitEthernet 1/0/1.10 to transmit broadcast and multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast enable
```

Configure GigabitEthernet 1/0/1.10 to tag a multicast or broadcast packet with each Layer 1 VLAN ID and each Layer 2 VLAN ID. The Layer 1 and Layer 2 VLAN IDs are in the range of 300 to 400 and 500 to 600, respectively.

Configure GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets whose Layer 1 and Layer 2 VLAN IDs are in the range of 300 to 400 and 500 to 600, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 300 to 400 second-dot1q 500 to 600
```

Enable GigabitEthernet 1/0/1.10 to transmit broadcast and multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast enable.
```

Configure VLAN-interface 10 to tag a multicast or broadcast packet with two layers of VLAN IDs. The Layer 1 VLAN ID is 10. The Layer 2 VLAN ID is each VLAN ID in the range of 10 to 20.

Configure VLAN-interface 10 to terminate VLAN-tagged packets with Layer 2 VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] second-dot1q 10 to 20
```

Enable VLAN-interface 10 to transmit broadcast and multicast packets.

```
[Sysname-Vlan-interface10] vlan-termination broadcast enable
```

vlan-termination broadcast ra

Use **vlan-termination broadcast ra** to enable an interface to transmit router advertisement (RA) multicast packets.

Use **undo vlan-termination broadcast ra** to disable an interface from transmitting RA multicast packets.

Syntax

vlan-termination broadcast ra

undo vlan-termination broadcast ra

Default

An ambiguous Dot1q or QinQ termination-enabled interface drops broadcast and multicast packets.

Views

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

To transmit an RA multicast packet, the interface starts a traversal over the VLAN IDs specified for ambiguous termination. It copies the packet and tags each copy with a VLAN ID, until all VLAN IDs in the specified range are traversed. For example, when ambiguous QinQ termination is configured, both layers of VLAN ID ranges are traversed.

As a best practice, use this command to enable an ambiguous Dot1q or QinQ termination-enabled interface to transmit RA multicast packets on an IPv6 network. This command prohibits transmission of broadcast packets and other types of multicast packets, and consumes less CPU resources than the **vlan-termination broadcast enable** command.

Examples

Configure GigabitEthernet 1/0/1.10 to tag RA multicast packets with each VLAN tag in the range of 10 to 20.

Enable Dot1q termination on GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 10 to 20
```

Enable GigabitEthernet 1/0/1.10 to transmit RA multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast ra
```

Configure GigabitEthernet 1/0/1.10 to tag RA multicast packets with each Layer 1 VLAN ID and each Layer 2 VLAN ID. The Layer 1 and Layer 2 VLAN IDs are in the range of 300 to 400 and 500 to 600, respectively.

Configure GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets whose Layer 1 and Layer 2 VLAN IDs are in the range of 300 to 400 and 500 to 600, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 300 to 400 second-dot1q 500 to 600
```

Enable GigabitEthernet 1/0/1.10 to transmit RA multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast ra
```

Configure VLAN-interface 10 to tag RA multicast packets with two layers of VLAN IDs. The Layer 1 VLAN ID is 10. The Layer 2 VLAN ID is each VLAN ID in the range of 10 to 20.

Configure VLAN-interface 10 to terminate VLAN-tagged packets with Layer 2 VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] second-dot1q 10 to 20
```

Enable VLAN-interface 10 to transmit RA multicast packets.

```
[Sysname-Vlan-interface10] vlan-termination broadcast ra
```

vlan-type dot1q default

Use **vlan-type dot1q default** to enable default termination on a subinterface.

Use **undo vlan-type dot1q default** to disable default termination on a subinterface.

Syntax

vlan-type dot1q default

undo vlan-type dot1q default

Default

Default termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Usage guidelines

This command enables the subinterface to process packets that cannot be terminated by other subinterfaces on the same main interface.

Examples

Enable default termination on GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q default
[Sysname-GigabitEthernet1/0/1.1] quit
```

vlan-type dot1q untagged

Use **vlan-type dot1q untagged** to enable untagged termination on a subinterface.

Use **undo vlan-type dot1q untagged** to disable untagged termination on a subinterface.

Syntax

vlan-type dot1q untagged

undo vlan-type dot1q untagged

Default

Untagged termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Usage guidelines

This command enables the subinterface to process untagged packets.

Examples

Enable untagged termination on GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q untagged
[Sysname-GigabitEthernet1/0/1.1] quit
```

vlan-type dot1q vid

Use **vlan-type dot1q vid** to enable Dot1q termination on a subinterface, and specify the outermost VLAN IDs in the VLAN-tagged packets that can be terminated by the subinterface.

Use **undo vlan-type dot1q vid** to disable Dot1q termination on a subinterface.

Syntax

vlan-type dot1q vid *vlan-id-list*

undo vlan-type dot1q vid *vlan-id-list*

Default

Dot1q termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 outermost VLAN ID items. Each item specifies an outermost VLAN ID or a range of outermost VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

The VLAN ID ranges specified by the *vlan-id-list* argument for different subinterfaces of a main interface cannot overlap.

Examples

Configure GigabitEthernet 1/0/1.1 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 2 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q vid 2 to 100
```

vlan-type dot1q vid second-dot1q

Use **vlan-type dot1q vid second-dot1q** to enable QinQ termination on a subinterface, and specify the outermost two layers of VLAN IDs of VLAN-tagged packets that can be terminated by the subinterface.

Use **undo vlan-type dot1q vid second-dot1q** to disable QinQ termination on a subinterface.

Syntax

vlan-type dot1q vid *vlan-id-list* **second-dot1q** { *vlan-id-list* | **any** }

undo vlan-type dot1q vid *vlan-id-list* **second-dot1q** { *vlan-id-list* | **any** }

Default

QinQ termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN ID items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

any: Specifies all values between 1 and 4094.

Usage guidelines

L2VE subinterfaces support only unambiguous QinQ termination, and do not support the **loose** keyword.

Two subinterfaces of the same Ethernet interface cannot terminate packets that include the same two layers of VLAN IDs. If you configure the subinterfaces to terminate the same Layer 1 VLAN ID, make sure their Layer 2 VLAN ID ranges do not overlap. If you specify both **any** and *vlan-id-list* as the respective Layer 2 VLAN ID ranges of the subinterfaces, the **any** keyword does not include the VLAN IDs specified by *vlan-id-list*.

Examples

Enable QinQ termination on the Layer 3 Ethernet subinterfaces, and configure each subinterface to terminate VLAN-tagged packets with the specified Layer 1 and Layer 2 VLAN IDs.

- Configure GigabitEthernet 1/0/1.1 to terminate VLAN-tagged packets whose Layer 1 and Layer 2 VLAN IDs are both 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q vid 100 second-dot1q 100
[Sysname-GigabitEthernet1/0/1.1] quit
```

- Configure GigabitEthernet 1/0/1.2 to terminate VLAN-tagged packets with Layer 1 VLAN ID 100 and Layer 2 VLAN IDs in the range of 200 to 300.

```
[Sysname] interface gigabitethernet 1/0/1.2
[Sysname-GigabitEthernet1/0/1.2] vlan-type dot1q vid 100 second-dot1q 200 to 300
[Sysname-GigabitEthernet1/0/1.2] quit
```

- Configure GigabitEthernet 1/0/1.3 to terminate VLAN-tagged packets whose Layer 1 VLAN ID is 100 and Layer 2 VLAN ID is any value between 1 and 4094.

```
[Sysname] interface gigabitethernet 1/0/1.3
[Sysname-GigabitEthernet1/0/1.3] vlan-type dot1q vid 100 second-dot1q any
[Sysname-GigabitEthernet1/0/1.3] quit
```

- Configure GigabitEthernet 1/0/1.4 to terminate VLAN-tagged packets whose Layer 1 VLAN ID is 100 and Layer 2 VLAN ID is in the range of 500 to 600.

```
[Sysname] interface gigabitethernet 1/0/1.4
[Sysname-GigabitEthernet1/0/1.4] vlan-type dot1q vid 100 second-dot1q 500 to 600
[Sysname-GigabitEthernet1/0/1.4] quit
```

- Configure GigabitEthernet 1/0/1.5 to terminate VLAN-tagged packets whose Layer 1 VLAN ID is 200 and Layer 2 VLAN ID is in the range of 500 to 600.

```
[Sysname] interface gigabitethernet 1/0/1.5
[Sysname-GigabitEthernet1/0/1.5] vlan-type dot1q vid 200 second-dot1q 500 to 600
[Sysname-GigabitEthernet1/0/1.5] quit
```

- Configure GigabitEthernet 1/0/1.6 to terminate VLAN-tagged packets whose Layer 1 VLAN ID is in the range of 300 to 400 and Layer 2 VLAN ID is 100.

```
[Sysname] interface gigabitethernet 1/0/1.6
[Sysname-GigabitEthernet1/0/1.6] vlan-type dot1q vid 300 to 400 second-dot1q 100
[Sysname-GigabitEthernet1/0/1.6] quit
```

- Configure GigabitEthernet 1/0/1.7 to terminate VLAN-tagged packets whose Layer 1 and Layer 2 IDs are in the range of 300 to 400 and 500 to 600, respectively.

  ```
  [Sysname] interface gigabitethernet 1/0/1.7
  [Sysname-GigabitEthernet1/0/1.7] vlan-type dot1q vid 300 to 400 second-dot1q 500 to 600
  [Sysname-GigabitEthernet1/0/1.7] quit
  ```

- Configure GigabitEthernet 1/0/1.8 to terminate VLAN-tagged packets with a Layer 1 VLAN ID in the range of 300 to 400 and any Layer 2 VLAN ID.

  ```
  [Sysname] interface gigabitethernet 1/0/1.8
  [Sysname-GigabitEthernet1/0/1.8] vlan-type dot1q vid 300 to 400 second-dot1q any
  ```

The following table describes the configuration results:

Layer 3 Ethernet subinterface	Layer 1 VLAN IDs of VLAN-tagged packets that the subinterface can terminate	Layer 2 VLAN IDs of VLAN-tagged packets that the subinterface can terminate
GigabitEthernet 1/0/1.1	100	100
GigabitEthernet 1/0/1.2	100	200–300
GigabitEthernet 1/0/1.3	100	1–99, 101–199, 301–499, and 601–4094
GigabitEthernet 1/0/1.4	100	500–600
GigabitEthernet 1/0/1.5	200	500–600
GigabitEthernet 1/0/1.6	300–400	100
GigabitEthernet 1/0/1.7	300–400	500–600
GigabitEthernet 1/0/1.8	300–400	1–99, 101–499, and 601–4094

Contents

PPP commands 1

PPP commands 1
display ip pool 2
display ppp access-user 3
display ppp compression iphc 8
ip address ppp-negotiate 11
ip pool 12
ip pool gateway 13
nas-port-type 13
ppp account-statistics enable 14
ppp authentication-mode 15
ppp chap password 16
ppp chap user 17
ppp compression iphc enable 17
ppp compression iphc rtp-connections 18
ppp compression iphc tcp-connections 19
ppp ipcp dns 20
ppp ipcp dns admit-any 21
ppp ipcp dns request 22
ppp ipcp remote-address match 22
ppp ip-pool route 23
ppp lcp delay 24
ppp pap local-user 24
ppp timer negotiate 25
remote address 26
remote address dhcp client-identifier 27
reset ppp access-user 28
reset ppp compression iphc 28
timer-hold 29
timer-hold retry 30

PPPoE commands 31

PPPoE server commands 31
display pppoe-server session packet 32
display pppoe-server session summary 34
display pppoe-server throttled-mac 35
display pppoe-server va-pool 37
ppp lcp echo mru verify 37
pppoe-server access-delay 38
pppoe-server access-line-id bas-info 39
pppoe-server access-line-id circuit-id parse-mode 40
pppoe-server access-line-id circuit-id trans-format 41
pppoe-server access-line-id content 42
pppoe-server access-line-id remote-id trans-format 43
pppoe-server access-line-id trust 44
pppoe-server bind 45
pppoe-server session-limit 45
pppoe-server session-limit per-mac 46
pppoe-server session-limit per-vlan 47
pppoe-server session-limit total 48
pppoe-server tag ac-name 49
pppoe-server tag ppp-max-payload 50
pppoe-server tag service-name 51
pppoe-server throttle per-mac 52
pppoe-server virtual-template va-pool 53
reset pppoe-server 54

PPPoE client commands 54
dialer bundle enable 56
dialer diagnose 56
dialer timer autodial 57
dialer timer idle 58
dialer-group 59
dialer-group rule 59
display pppoe-client session packet 61
display pppoe-client session summary 62
mtu 63
pppoe-client 63
reset pppoe-client 64
reset pppoe-client session packet 65

PPP commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

PPP commands

The following compatibility matrix shows the support of hardware platforms for PPP:

Hardware series	Model	Product code	PPP compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X-PWR • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT	Yes

Hardware series	Model	Product code	PPP compatibility
	LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	PPP compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

display ip pool

Use **`display ip pool`** to display PPP address pools.

Syntax

`display ip pool` [*`pool-name`* | **`group`** *`group-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`pool-name`: Specifies a PPP address pool by its name, a case-sensitive string of 1 to 31 characters.

`group` *`group-name`*: Displays PPP address pools in a group specified by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays brief information about all PPP address pools.

If you specify an address pool, the command displays detailed information about the specified PPP address pool.

Examples

Display brief information about all PPP address pools.

```
<Sysname> display ip pool
Group name: a
  Pool name           Start IP address    End IP address      Free   In use
  aaa1                1.1.1.1             1.1.1.5             5      0
  aaa2                1.1.1.6             1.1.1.10            5      0
Group name: b
```

```
  Pool name           Start IP address    End IP address      Free   In use
  bbb                 1.1.2.1             1.1.2.5             4      1
                      2.2.2.1             2.2.2.5             5      0
```

Display brief information about the PPP address pools in group **a**.

```
<Sysname> display ip pool group a
Group name: a
  Pool name           Start IP address    End IP address      Free   In use
  aaa1                1.1.1.1             1.1.1.5             5      0
  aaa2                1.1.1.6             1.1.1.10            5      0
```

Display detailed information about PPP address pool **bbb**.

```
<Sysname> display ip pool bbb
Group name: b
  Pool name           Start IP address    End IP address      Free   In use
  bbb                 1.1.2.1             1.1.2.5             4      1
                      2.2.2.1             2.2.2.5             5      0
In use IP addresses:
  IP address      Interface
  1.1.2.1         Virtual-Template1
```

Table 1 Command output

Field	Description
Free	Number of free IP addresses.
In use	Number of IP addresses that have been assigned.
In use IP addresses	Information about the IP addresses that have been assigned.
Interface	Local interface that requests the IP address for the peer interface.

Related commands

ip pool

display ppp access-user

Use **display ppp access-user** to display PPP user information.

Syntax

display ppp access-user { **interface** *interface-type interface-number* [**count**] | **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address*| **username** *user-name* | **user-type** { **lac** | **lns** | **pppoe** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays brief information about PPP users on the specified interface.

ip-address *ipv4-address*: Displays detailed information about the PPP user specified by its IPv4 address.

ipv6-address *ipv6-address*: Displays detailed information about the PPP user specified by its IPv6 address.

username *user-name*: Displays detailed information about the PPP user specified by its username, a case-sensitive string of 1 to 80 characters.

user-type: Displays brief information about online users of the specified type.

lac: Displays brief information about L2TP users for an LAC.

lns: Displays brief information about L2TP users for an LNS.

pppoe: Displays brief information about PPPoE users.

count: Displays the total number of PPP users matching the specified criterion.

Usage guidelines

Brief information about a PPP user includes the following:

- Brief name of the VA interface.
- Username.
- MAC address.
- IPv4 address, IPv6 address, or IPv6 prefix of the PPP user.

Detailed information about a PPP user includes the following:

- Brief name of the VA interface.
- User ID.
- Username.
- Authentication information.
- Uplink and downlink traffic.
- Access start time of the PPP user.

In an L2TP network, this command is supported on an LAC only if a remote system dials in to the LAC through a PPPoE network. For more information about L2TP, see L2TP configuration in *Network Connectivity Configuration Guide*.

Examples

Display brief information about PPP users on GigabitEthernet 1/0/1.

```
<Sysname> display ppp access-user interface gigabitethernet 1/0/1
Interface     Username    MAC address     IP address       IPv6 address    IPv6 PDPrefix
VA0           user1@dm1   0001-0101-9101  192.168.100.173  -                 -
VA1           user2@dm2   0001-0101-9101  192.168.80.173   2000::1           -
```

Display the total number of PPP users on GigabitEthernet 1/0/1.

```
<Sysname> display ppp access-user interface gigabitethernet 1/0/1 count
Total users: 2
```

Table 2 Command output

Field	Description
Interface	Name of the VA interface corresponding to the user.
Username	Username of the user. A hyphen (-) means that the user does not need authentication.
MAC address	MAC address of the user.

Field	Description
	A hyphen (-) means that the user is not a PPPoE user.
IP address	IP address of the user. A hyphen (-) means that no IP address is assigned to the user.
IPv6 address	IPv6 address of the user. A hyphen (-) means that no IPv6 address is assigned to the user.
IPv6 PD prefix	IPv6 prefix of the user. A hyphen (-) means that no IPv6 prefix is assigned to the user.
Total users	Total number of PPP users.

Display detailed information about the PPP user whose IP address is 50.50.50.3.

```
<Sysname> display ppp access-user ip-address 50.50.50.3
Basic:
  Interface: VA0
  User ID: 0x28000002
  Username: user1@hrss
  Domain: hrss
  Access interface: RAGG2
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  IP address: 50.50.50.3
  IPv6 address: -
  IPv6 PD prefix: -
  VPN instance: 123
  Access type: PPPoE
  Authentication type: CHAP

AAA:
  Authentication state: Authenticated
  Authorization state: Authorized
  Realtime accounting switch: Open
  Realtime accounting interval: 60s
  Login time: 2013-1-19  2:42:3:358
  Accounting start time: 2013-1-19  2:42:3:382
  Online time(hh:mm:ss): 0:7:34
  Accounting state: Accounting
  Idle cut: 0 sec  0 byte
  Session timeout: 12000 s
  Time remained: 8000 s
  Byte remained: 20971520 bytes
  Redirect WebURL: http://6.6.6.6

ACL&QoS:
  User profile: profile123 (active)
  User group profile: -
  Inbound CAR: CIR 64000bps PIR 640000bps CBS 500bit
  Outbound CAR: CIR 64000bps PIR 640000bps CBS 500bit
```

```
NAT:
  Global IP address: 111.8.0.200
  Port block: 28744-28748

Flow Statistic:
  IPv4 uplink   packets/bytes: 7/546
  IPv4 downlink packets/bytes: 0/0
  IPv6 uplink   packets/bytes: 0/0
  IPv6 downlink packets/bytes: 0/0

ITA:
  Level-1 uplink   packets/bytes: 100/128000
          downlink packets/bytes: 200/256000
  Level-2 uplink   packets/bytes: 100/128000
          downlink packets/bytes: 200/256000
```

Table 3 Command output

Field	Description
Basic	Basic information.
Interface	Brief name of the VA interface that corresponds to the user.
Username	Username of the user. A hyphen (-) means that the user does not need authentication.
Domain	ISP domain name for authentication. A hyphen (-) means that no ISP domain is specified for authentication.
Access interface	Name of the access interface of the user.
Service-VLAN/Customer-VLAN	Service provider VLAN and customer VLAN information of the user. A hyphen (-) means that no VLAN information is available.
IP address	IP address of the user. A hyphen (-) means that no IP address is assigned to the user.
IPv6 address	IPv6 address of the user. A hyphen (-) means that no IPv6 address is assigned to the user.
IPv6 PD prefix	Delegated IPv6 prefix of the user. A hyphen (-) means that no delegated IPv6 prefix is assigned to the user.
VPN instance	This field is not supported in the current software version.VPN instance to which the user belongs. A hyphen (-) means that the user is not bound to any VPN instance.
Access type	Access type of the user: • PPPoE. • L2TP.
Authentication type	Authentication type of the user: 用户接入采用的认证类型，包括：PAP、CHAP
Authentication state	Authentication state of the user: • **Idle**—The user has not been authenticated. • **Authenticating**—The user is being authenticated.

Field	Description
	• **Authenticated**—The user has been authenticated.
Authorization state	Authorization state of the user: • **Idle**—The user has not been authorized. • **Authorizing**—The user is being authorized. • **Authorized**—The user has been authorized.
Realtime accounting switch	• **Open**—The switch is on. • **Closed**—The switch is off.
Realtime accounting interval	Realtime accounting interval in seconds. A hyphen (-) means that no real-time accounting interval is authorized.
Login time	Time when the user accessed the device through PPP.
Accounting start time	Time when accounting started. A hyphen (-) means that no accounting is performed on the user.
Online time(hh:mm:ss)	Online duration of the current login.
Accounting state	Accounting state of the user: • **Accounting**—Accounting is on. • **Stop**—Accounting stops.
Idle cut	Traffic threshold for logging off the user in idle state. If the traffic is less than the threshold within the specified period, the user is forcibly logged off.
Session timeout	Authorization time for the user, in seconds. A hyphen (-) means that no authorization time is specified for the user.
Time remained	Remaining time for the user to stay online, in seconds. A hyphen (-) means that no authorization time is specified for the user.
Byte remained	Remaining traffic for the user. A hyphen (-) means that no authorization traffic is specified for the user.
Redirect WebURL	Redirect Web URL address for the user. A hyphen (-) means that no redirect Web URL address is specified for the user.
User profile	Name of the authorized user profile. The hyphen (-) means that no user profile is authorized. The user profile has two states: • **active**—The authorized user profile is successfully issued. • **inactive**—The authorized user profile fails to be issued.
User group profile	Name of the authorized user group profile. The hyphen (-) means that no user group profile is authorized. The user group profile has two states: • **active**—The authorized user group profile is successfully issued. • **inactive**—The authorized user group profile fails to be issued.
Inbound CAR	Authorized inbound CAR parameters, which contain the CIR (in bps), the PIR (in bps), and the CBS (in bits).

Field	Description
Outbound CAR	Authorized outbound CAR parameters, which contain the CIR (in bps), the PIR (in bps), and the CBS (in bits).
Global IP address	Global IP address of the user. This field is displayed if NAT444 is used. For information about NAT444, see *Network Connectivity Configuration Guide*.
Port block	Port block of the user, from the start port to the end port. This field is displayed if NAT444 is used.
IPv4 uplink packets/bytes	Number of packets and bytes for IPv4 uplink traffic.
IPv4 downlink packets/bytes	Number of packets and bytes for IPv4 downlink traffic.
IPv6 uplink packets/bytes	Number of packets and bytes for IPv6 uplink traffic.
IPv6 downlink packets/bytes	Number of packets and bytes for IPv6 downlink traffic.
ITA	ITA statistics. ITA statistics are displayed after ITA is enabled. If the **traffic-separate enable** command is configured, ITA statistics are not included in flow statistics. For information about ITA and the **traffic-separate enable** command, see *User Access and Authentication Configuration Guide*.
Level-n uplink packets/bytes downlink packets/bytes	Number of packets and bytes for uplink traffic at accounting level *n*. The value for *n* depends on the **traffic level** command, and its value range is 1 to 8.

Related commands

reset ppp access-user

display ppp compression iphc

Use **display ppp compression iphc** to display IP header compression (IPHC) statistics.

Syntax

display ppp compression iphc { **rtp** | **tcp** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

rtp: Displays IPHC RTP header compression statistics.

tcp: Displays IPHC TCP header compression statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays IPHC statistics on all interfaces.

Usage guidelines

When IPHC applies to a normal PPP link, the physical interface performs IPHC. You can view the compression information on the physical interface.

Examples

(In standalone mode.) Display IPHC RTP header compression statistics.

```
<Sysname> display ppp compression iphc rtp
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

(In standalone mode.) Display IPHC TCP header compression statistics.

```
<Sysname> display ppp compression iphc tcp
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

(In IRF mode.) Display IPHC RTP header compression statistics.

```
<Sysname> display ppp compression iphc rtp
----------------------Slot1----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0

----------------------Slot2----------------------
Interface: Virtual-Access0
  Received:
```

```
    Compressed/Error/Total: 20/5/40 packets
  Sent:
    Compressed/Total: 34/40 packets
    Sent/Saved/Total: 1131/1210/2341 bytes
    Packet-based compression ratio: 85%
    Byte-based compression ratio: 51%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

(In IRF mode.) Display IPHC TCP header compression statistics.

```
<Sysname>display ppp compression iphc tcp
----------------------Slot1----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0

----------------------Slot2----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 20/5/40 packets
  Sent:
    Compressed/Total: 34/40 packets
    Sent/Saved/Total: 1131/1210/2341 bytes
    Packet-based compression ratio: 85%
    Byte-based compression ratio: 51%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

Table 4 Command output

Field	Description
Received: Compressed/Error/Total	Statistics for received packets: • **Compressed**—Number of compressed packets. • **Error**—Number of error packets. • **Total**—Total number of received packets.
Sent: Compressed/Total	Statistics for sent packets: • **Compressed**—Number of compressed packets.

Field	Description
Sent/Saved/Total Packet-based compression ratio Byte-based compression ratio	• **Total**—Total number of sent packets. • **Sent**—Bytes of sent packets. • **Saved**—Bytes of saved packets. • **Total**—Total bytes to be sent if packets are not compressed. • **Packet-based compression ratio**—Ratio of compressed packets to the total sent packets. • **Byte-based compression ratio**—Ratio of saved bytes to the total sent bytes.
Connections: Rx/Tx Five-Minute-Miss Max-Miss	Number of connections. • **Rx**—Number of connections that the receiver can decompress. • **Tx**—Number of connections that the sender can compress. • **Five-Minute-Miss**—Number of search failures within the last 5 minutes. • **Max-Miss**—Maximum number of search failures within 5 minutes.

Related commands

ppp compression iphc enable

reset ppp compression iphc

ip address ppp-negotiate

Use **ip address ppp-negotiate** to enable IP address negotiation on an interface, so that the interface can accept the IP address allocated by the server.

Use **undo ip address ppp-negotiate** to restore the default.

Syntax

ip address ppp-negotiate

undo ip address ppp-negotiate

Default

IP address negotiation is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If you execute the **ip address ppp-negotiate** and **ip address** commands multiple times, the most recent configuration takes effect.

Examples

Enable IP address negotiation on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ip address ppp-negotiate
```

Related commands

ip address (*Network Connectivity Command Reference*)

remote address

ip pool

Use **ip pool** to configure a PPP address pool.

Use **undo ip pool** to remove a PPP address pool or an IP address range of the PPP address pool.

Syntax

ip pool *pool-name start-ip-address* [*end-ip-address*] [**group** *group-name*]

undo ip pool *pool-name* [*start-ip-address* [*end-ip-address*]]

Default

No PPP address pool is configured.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a name for the PPP address pool to be created, a case-sensitive string of 1 to 31 characters.

start-ip-address [*end-ip-address*]: Specifies an IP address range. If you do not specify the *end-ip-address* argument, the PPP address pool has only the start IP address.

group *group-name*: Specifies a group by its name to which the PPP address pool belongs. The group name is a case-sensitive string of 1 to 31 characters. If you do not specify this option, the group name is **default** (the default group).

Usage guidelines

Each address space is represented by a group. One group can contain multiple PPP address pools, but one PPP address pool can belong to only one group.

One PPP address pool can contain multiple IP address ranges. You can execute this command multiple times to specify multiple IP address ranges for a PPP address pool. A PPP address pool can contain a maximum of 65535 IP addresses, and so can an IP address range.

IP address ranges in different groups can be overlapping, but those in the same group cannot.

Changes to a PPP address pool do not affect assigned IP addresses. For example, if you delete a PPP address pool from which an IP address has been assigned, the IP address can still be used.

When assigning IP address to users through a PPP address pool, make sure the PPP address pool excludes the gateway IP address of the PPP address pool.

Examples

Configure PPP address pool **aaa** that contains IP addresses 129.102.0.1 through 129.102.0.10 for group **a**.

```
<Sysname> system-view
[Sysname] ip pool aaa 129.102.0.1 129.102.0.10 group a
```

Related commands

display ip pool

ip pool gateway

Use **ip pool gateway** to configure a gateway address for a PPP address pool.

Use **undo ip pool gateway** to remove the gateway address for the specified PPP address pool.

Syntax

ip pool *pool-name* **gateway** *ip-address*

undo ip pool *pool-name* **gateway**

Default

A PPP address pool is not configured with a gateway address.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies an existing PPP address pool by its name, a case-sensitive string of 1 to 31 characters.

ip-address: Specifies a gateway address for the PPP address pool.

Usage guidelines

An interface on a BRAS must have an IP address before it can assign an IP address from a PPP or DHCP address pool to a client. This command enables interfaces that have no IP address to use a gateway address for IPCP negotiation and address allocation.

When you configure a gateway address for a PPP address pool, follow these restrictions and guidelines:

- If you also specify an IP address for an interface, the interface uses its own IP address to perform IPCP negotiation.
- You can specify any gateway address for a PPP address pool.

Examples

Specify gateway address **1.1.1.1** for PPP address pool **aaa**.

```
<Sysname> system-view
[Sysname] ip pool aaa gateway 1.1.1.1
```

Related commands

ip pool

nas-port-type

Use **nas-port-type** to configure the NAS-Port-Type attribute on a VT interface.

Use **undo nas-port-type** to restore the default.

Syntax

nas-port-type { **ethernet** | **virtual** }

undo nas-port-type

Default

The NAS-Port-Type attribute is determined by the service type and link type of the PPP user, as shown in Table 5.

Table 5 Default NAS-Port-Type attribute

Service type	Link type	NAS-Port-Type attribute
PPPoE	Any	**ethernet**
L2TP	Any	**virtual**

Views

VT interface view

Predefined user roles

network-admin

Parameters

ethernet: Specifies Ethernet. The code value is 15.

virtual: Specifies virtual. The code value is 5.

Usage guidelines

The NAS-Port-Type attribute is used for RADIUS authentication and accounting. For more information about the NAS-Port-Type attribute, see RFC 2865.

This command does not affect existing users.

Examples

Set the NAS-Port-Type attribute to **ethernet** for Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] nas-port-type ethernet
```

ppp account-statistics enable

Use **ppp account-statistics enable** to enable PPP accounting on an interface.

Use **undo ppp account-statistics enable** to disable PPP accounting on an interface.

Syntax

ppp account-statistics enable [**acl** { *acl-number* | **name** *acl-name* }]

undo ppp account-statistics enable

Default

PPP accounting is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl: Specifies an ACL to match traffic. If no ACL is specified, the device generates statistics for all PPP traffic.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999, where:

- 2000 to 2999 are numbers for basic IPv4 and IPv6 ACLs.
- 3000 to 3999 are numbers for advanced IPv4 and IPv6 ACLs.

If the specified ACL number corresponds to an IPv4 ACL and an IPv6 ACL, both ACLs take effect.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters that start with an alphabetical character. To avoid confusion, do not use **all** as an ACL name.

Examples

Enable PPP accounting on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp account-statistics enable
```

ppp authentication-mode

Use **ppp authentication-mode** to configure PPP authentication on an interface.

Use **undo ppp authentication-mode** to restore the default.

Syntax

ppp authentication-mode { **chap** | **pap** } * [[**call-in**] **domain** { *isp-name* | **default enable** *isp-name* }]

undo ppp authentication-mode

Default

PPP authentication is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

chap: Uses CHAP authentication.

pap: Uses PAP authentication.

call-in: Authenticates the call-in users only.

domain *isp-name*: Specifies the ISP domain name for authentication, a case-insensitive string of 1 to 255 characters.

default enable *isp-name*: Specifies the default ISP domain name for authentication, a case-insensitive string of 1 to 255 characters.

Usage guidelines

PPP authentication includes the following categories:

- **PAP**—Two-way handshake authentication. The password is in plain text or cipher text.
- **CHAP**—Three-way handshake authentication. The password is in plain text or cipher text.

You can configure multiple authentication modes.

In any PPP authentication mode, AAA determines whether a user can pass the authentication through a local authentication database or an AAA server. For more information about AAA authentication, see *User Access and Authentication Configuration Guide*.

If multiple ISP domains are available, the ISP domains are used in the following order:

1. ISP domain specified by the **domain** *isp-name* option in this command.

   Associate a PPP address pool with this ISP domain for address allocation if necessary.
2. ISP domain contained in the username.

   If the ISP domain does not exist on the local device, the user's access request is denied.
3. ISP domain specified by the **domain default enable** *isp-name* option in this command.
4. Default system ISP domain.

   You can use the **domain default** command to configure the default system ISP domain. If no system default ISP domain is configured, ISP domain **system** is used.

Examples

Configure Virtual-Template 1 to authenticate the peer by using PAP.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode pap
```

Configure Virtual-Template 1 to authenticate the peer by using PAP and CHAP.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode pap chap
```

Related commands

domain default (*User Access and Authentication Command Reference)*

local-user (*User Access and Authentication Command Reference)*

ppp chap password

ppp chap user

ppp pap local-user

ppp chap password

Use **ppp chap password** to set the password for CHAP authentication on an interface.

Use **undo ppp chap password** to restore the default.

Syntax

ppp chap password { **cipher** | **simple** } *string*

undo ppp chap password

Default

No password is set for CHAP authentication on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 1 to 373 characters.

Examples

Set the password for CHAP authentication to plaintext password **sysname** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp chap password simple sysname
```

Related commands

ppp authentication-mode chap

ppp chap user

Use **ppp chap user** to set the username for CHAP authentication on an interface.

Use **undo ppp chap user** to restore the default.

Syntax

ppp chap user *username*

undo ppp chap user

Default

The username for CHAP authentication is null on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

username: Specifies the username for CHAP authentication, a case-sensitive string of 1 to 80 characters. The username is sent to the peer for the local device to be authenticated.

Usage guidelines

To pass CHAP authentication, the username/password of one side must be the local username/password on the peer.

Examples

Set the username for CHAP authentication to **Root** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp chap user Root
```

Related commands

ppp authentication-mode chap

ppp compression iphc enable

Use **ppp compression iphc enable** to enable IPHC on an interface.

Use **undo ppp compression iphc enable** to disable IPHC on an interface.

Syntax

ppp compression iphc enable [**nonstandard**]

undo ppp compression iphc enable

Default

IPHC is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

nonstandard: Specifies the nonstandard encapsulation format. If you do not specify this keyword, packets are encapsulated in standard format. You must specify this keyword when the device communicates with a non-H3C device. If you specify this keyword, this command enables RTP header compression.

Usage guidelines

IPHC includes RTP header compression and TCP header compression.

Enabling or disabling IPHC enables or disables both RTP header compression and TCP header compression.

To use IPHC, you must enable it on both sides of a PPP link.

When you enable IPHC on a VT or dialer interface, the setting does not immediately take effect. For the setting to take effect, execute the **shutdown** and then **undo shutdown** commands on the interface or its bound physical interface.

Examples

Enable IPHC on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
```

ppp compression iphc rtp-connections

Use **ppp compression iphc rtp-connections** to set the maximum number of connections for which an interface can perform RTP header compression.

Use **undo ppp compression iphc rtp-connections** to restore the default.

Syntax

ppp compression iphc rtp-connections *number*

undo ppp compression iphc rtp-connections

Default

An interface can perform RTP header compression for a maximum of 16 connections.

Views

Interface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of connections for which an interface can perform RTP header compression. The value range for this argument is 3 to 1000:

- When the *number* argument is set to a value less than or equal to 256, packets are compressed in the format of COMPRESSED RTP 8.
- When the *number* argument is set to a value greater than 256, packets are compressed in the format of COMPRESSED RTP 16.

Usage guidelines

RTP is a connection-oriented protocol. An interface can accommodate multiple RTP connections.

RTP header compression occupies memory resources for maintaining connection information. This command can limit memory resources used by compression. For example, if you set the limit to 3, RTP header compression only applies to a maximum of three RTP connections.

After you execute this command, you must shut down and then bring up the interface to make the command take effect.

You can configure this command only when IPHC is enabled. The configuration is removed after IPHC is disabled.

Examples

Set the maximum number of connections for which Virtual-Template 1 can perform RTP header compression to 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
[Sysname-Virtual-Template1] ppp compression iphc rtp-connections 10
```

Related commands

ppp compression iphc enable

ppp compression iphc tcp-connections

Use **ppp compression iphc tcp-connections** to set the maximum number of connections for which an interface can perform TCP header compression.

Use **undo ppp compression iphc tcp-connections** to restore the default.

Syntax

ppp compression iphc tcp-connections *number*

undo ppp compression iphc tcp-connections

Default

An interface can perform TCP header compression for a maximum of 16 connections.

Views

Interface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of connections for which an interface can perform TCP header compression. The value range for this argument is 3 to 256.

Usage guidelines

TCP is a connection-oriented protocol. A link can accommodate multiple TCP connections.

TCP header compression occupies memory resources for maintaining connection information. This command can limit memory resources used by compression. For example, if you set the limit to 3, TCP header compression only applies to a maximum of three TCP connections.

After you execute this command, you must shut down and then bring up the interface to make the command take effect.

You can configure this command only when IPHC is enabled and packets are encapsulated in standard format. The configuration is removed after IPHC is disabled or packets are encapsulated in nonstandard format.

Examples

Set the maximum number of connections for which Virtual-Template 1 can perform TCP header compression to 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
[Sysname-Virtual-Template1] ppp compression iphc tcp-connections 10
```

Related commands

ppp compression iphc enable

ppp ipcp dns

Use **ppp ipcp dns** to configure the primary and secondary DNS server IP addresses to be allocated in PPP negotiation on an interface.

Use **undo ppp ipcp dns** to delete the primary and secondary DNS server IP addresses to be allocated in PPP negotiation on an interface.

Syntax

ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

undo ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

Default

The DNS server IP addresses to be allocated in PPP negotiation are not configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

primary-dns-address: Specifies a primary DNS server IP address.

secondary-dns-address: Specifies a secondary DNS server IP address.

Usage guidelines

A device can assign DNS server IP addresses to its peer during PPP negotiation when the peer initiates requests.

To check the allocated DNS server IP addresses, execute the **winipcfg** or **ipconfig /all** command on the host.

Examples

Set the primary and secondary DNS server IP addresses to 100.1.1.1 and 100.1.1.2 for the peer on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns 100.1.1.1 100.1.1.2
```

ppp ipcp dns admit-any

Use **ppp ipcp dns admit-any** to configure an interface to accept the DNS server IP addresses assigned by the peer even though it does not request DNS server IP addresses from the peer.

Use **undo ppp ipcp dns admit-any** to restore the default.

Syntax

ppp ipcp dns admit-any

undo ppp ipcp dns admit-any

Default

An interface does not accept the DNS server IP addresses assigned by the peer if it does not request DNS server IP addresses from the peer.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

You can configure an interface to accept the DNS server IP addresses assigned by the peer, through which domain names can be resolved for the device.

Typically, the server assigns a DNS server address to a client in PPP negotiation only when the client is configured with the **ppp ipcp dns request** command. Some servers, however, forcibly assign DNS server addresses to clients. You must configure the **ppp ipcp dns admit-any** command on the client devices to accept the DNS server addresses.

Examples

Configure Virtual-Template 1 to accept DNS server IP addresses allocated by the peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns admit-any
```

Related commands

ppp ipcp dns request

ppp ipcp dns request

Use **ppp ipcp dns request** to enable an interface to actively request the DNS server IP address from its peer.

Use **undo ppp ipcp dns request** to restore the default.

Syntax

ppp ipcp dns request

undo ppp ipcp dns request

Default

An interface does not actively request the DNS server IP address from its peer.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If a device is connected to a provider's access server through a PPP link, you can use this command. Then, the device can obtain the specified DNS server IP address from the access server during IPCP negotiation.

You can check the DNS server IP addresses by displaying information about the interface.

Examples

Enable Virtual-Template 1 to actively request the DNS server IP address from its peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns request
```

ppp ipcp remote-address match

Use **ppp ipcp remote-address match** to enable the IP segment match feature for PPP IPCP negotiation on an interface.

Use **undo ppp ipcp remote-address match** to restore the default.

Syntax

ppp ipcp remote-address match

undo ppp ipcp remote-address match

Default

The IP segment match feature is disabled for PPP IPCP negotiation on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the local interface to check whether its IP address and the IP address of the remote interface are in the same network segment. If they are not, IPCP negotiation fails.

Examples

Enable the IP segment match feature on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] ppp ipcp remote-address match
```

ppp ip-pool route

Use **ppp ip-pool route** to configure a PPP address pool route.

Use **undo ppp ip-pool route** to remove a PPP address pool route.

Syntax

ppp ip-pool route *ip-address* { *mask-length* | *mask* }

undo ppp ip-pool route *ip-address* { *mask-length* | *mask* }

Default

No PPP address pool route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the PPP address pool route, in dotted decimal notation.

mask-length: Specifies a mask length for the IP address, in the range of 0 to 32.

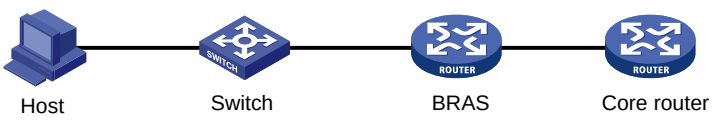
mask: Specifies a mask for the IP address, in dotted decimal notation.

Usage guidelines

The BRAS uses PPP address pool routes to control downlink traffic forwarding.

After you configure a PPP address pool route, the BRAS generates a static blackhole route destined for the specified network. All traffic matching the blackhole route is discarded. When a legal user logs in, the BRAS adds a host route destined for the specified network. In addition, the BRAS uses a dynamic routing protocol to redistribute the PPP address pool route to the upstream device.

Figure 1 Network diagram for the PPP address pool route



Make sure the destination network of the PPP address pool route includes the PPP address pool. You can execute this command multiple times to configure multiple PPP address pool routes.

Examples

Configure the PPP address pool route as 2.2.2.2/24.

```
<Sysname> system-view
[Sysname] ppp ip-pool route 2.2.2.2 24
```

ppp lcp delay

Use **ppp lcp delay** to set the LCP negotiation delay timer.

Use **undo ppp lcp delay** to restore the default.

Syntax

ppp lcp delay *milliseconds*

undo ppp lcp delay

Default

PPP starts LCP negotiation immediately after the physical layer comes up.

Views

Interface view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the LCP negotiation delay timer in the range of 1 to 10000 milliseconds.

Usage guidelines

If two ends of a PPP link vary greatly in the LCP negotiation packet processing rate, configure this command on the end with a higher processing rate. The LCP negotiation delay timer prevents frequent LCP negotiation packet retransmission. After the physical layer comes up, PPP starts LCP negotiation when the delay timer expires. If PPP receives LCP negotiation packets before the delay timer expires, it starts LCP negotiation immediately.

Examples

Set the LCP negotiation delay timer to 130 milliseconds.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp delay 130
```

ppp pap local-user

Use **ppp pap local-user** to set the local username and password for PAP authentication on an interface.

Use **undo ppp pap local-user** to restore the default.

Syntax

ppp pap local-user *username* **password** { **cipher** | **simple** } *string*

undo ppp pap local-user

Default

The local username and password for PAP authentication are blank on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

username: Specifies the username of the local device for PAP authentication, a case-sensitive string of 1 to 80 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 1 to 373 characters.

Usage guidelines

For the local device to pass PAP authentication on the peer, make sure the username and password configured for the local device are also configured on the peer. You can configure the peer's username and password by using the **local-user** *username* and **password** { **cipher** | **simple** } *string* commands, respectively.

Examples

Set the local username and password for PAP authentication to **user1** and plaintext **pass1** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp pap local-user user1 password simple pass1
```

Related commands

local-user (*User Access and Authentication Command Reference*)

password (*User Access and Authentication Command Reference*)

ppp timer negotiate

Use **ppp timer negotiate** to set the PPP negotiation timeout time on an interface.

Use **undo ppp timer negotiate** to restore the default.

Syntax

ppp timer negotiate *seconds*

undo ppp timer negotiate

Default

The PPP negotiation timeout time is 3 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the negotiation timeout time in the range of 1 to 10 seconds.

Usage guidelines

In PPP negotiation, if the local device receives no response from the peer during the timeout time after it sends a packet, the local device sends the last packet again.

Examples

Set the PPP negotiation timeout time to 5 seconds on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp timer negotiate 5
```

remote address

Use **remote address** to configure an interface to assign an IP address to the client.

Use **undo remote address** to restore the default.

Syntax

remote address { *ip-address* | **pool** *pool-name* }

undo remote address

Default

An interface does not assign an IP address to the client.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be assigned to the client.

pool *pool-name*: Specifies a PPP or DHCP address pool by its name from which an IP address is assigned to the client. The pool name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command can be used when the local interface is configured with an IP address, but the peer has no IP address. To enable the peer to accept the IP address assigned by the local interface (server), you must configure the **ip address ppp-negotiate** command on the peer to make the peer act as a client.

This command enables the local interface to forcibly assign an IP address to the peer. If the peer is not configured with the **ip address ppp-negotiate** command but configured with an IP address, the peer will not accept the assigned IP address. This results in an IPCP negotiation failure.

PPP supports IP address assignment from a PPP or DHCP address pool, but the PPP address pool takes precedence over the DHCP address pool. For example, if you use a pool name that identifies both a PPP address pool and a DHCP address pool, the system uses only the PPP address pool for address assignment.

To make the configuration of the **remote address** command take effect, configure this command before the **ip address** command, which triggers IPCP negotiation. If you configure the **remote address** command after the **ip address** command, the server assigns an IP address to the client during the next IPCP negotiation.

After you use the **remote address** command to assign an IP address to the client, you can configure the **remote address** command again or the **undo remote address** command for the peer. However, the new configuration does not take effect until the next IPCP negotiation.

Examples

Specify the IP address to be assigned to the client as 10.0.0.1 on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address 10.0.0.1
```

Configure Virtual-Template 1 to assign an IP address from address pool **aaa** to the client.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address pool aaa
```

Related commands

ip address ppp-negotiate

ip pool

remote address dhcp client-identifier

Use **remote address dhcp client-identifier username** to use the PPP usernames as the DHCP client IDs.

Use **undo remote address dhcp client-identifier** to restore the default.

Syntax

remote address dhcp client-identifier username

undo remote address dhcp client-identifier

Default

The PPP usernames are not used as the DHCP client IDs.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command uses PPP usernames as DHCP client IDs for DHCP pool address assignment. The DHCP pool can be an AAA-authorized address pool or an address pool configured by using the **remote address** command.

Configure this command when different users use different PPP usernames to come online and PPP usernames are required to be used as DHCP client IDs.

Examples

Use the PPP usernames as the DHCP client IDs on Virtual-template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address dhcp client-identifier username
```

reset ppp access-user

Use **reset ppp access-user** to log off a PPP user.

Syntax

reset ppp access-user { **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **username** *user-name* }

Views

User view

Predefined user roles

network-admin

Parameters

ip-address *ipv4-address*: Specifies a PPP user by its IPv4 address.

ipv6-address *ipv6-address*: Specifies a PPP user by its IPv6 address.

username *user-name*: Specifies a PPP user by username, a case-sensitive string of 1 to 80 characters.

Usage guidelines

This command takes effect only on the current login for a PPP user. The user can come online after it is logged off.

Examples

Log off the PPP user at 192.168.100.2.

```
<Sysname> reset ppp access-user ip-address 192.168.100.2
```

Related commands

display ppp access-user

reset ppp compression iphc

Use **reset ppp compression iphc** to clear IPHC statistics.

Syntax

reset ppp compression iphc [**rtp** | **tcp**] [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

rtp: Clears IPHC RTP header compression statistics.

tcp: Clears IPHC TCP header compression statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command clears IPHC statistics on all interfaces.

Usage guidelines

If neither **rtp** nor **tcp** is specified, this command clears both RTP header compression and TCP header compression statistics.

Examples

Clear IPHC statistics on all interfaces.

```
<Sysname> reset ppp compression iphc
```

Related commands

display ppp compression iphc

timer-hold

Use **timer-hold** to set the keepalive interval on an interface.

Use **undo timer-hold** to restore the default.

Syntax

timer-hold *seconds*

undo timer-hold

Default

The keepalive interval is 10 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the interval for sending keepalive packets, in the range of 0 to 32767 seconds. The value 0 disables an interface from sending keepalive packets. In this case, the interface can respond to keepalive packets from the peer.

Usage guidelines

An interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface receives no response to keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive retry limit, use the **timer-hold retry** command.

On a slow link, increase the keepalive interval to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive interval to 20 seconds on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] timer-hold 20
```

Related commands

timer-hold retry

timer-hold retry

Use **timer-hold retry** to set the keepalive retry limit on an interface.

Use **undo timer-hold retry** to restore the default.

Syntax

timer-hold retry *retries*

undo timer-hold retry

Default

The keepalive retry limit is 5 on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of keepalive attempts in the range of 1 to 255.

Usage guidelines

An interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface receives no response to keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive interval, use the **timer-hold** command.

On a slow link, increase the keepalive retry limit to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive retry limit to 10 for Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] timer-hold retry 10
```

Related commands

timer-hold

PPPoE commands

PPPoE server commands

The following compatibility matrix shows the support of hardware platforms for PPPoE server:

Hardware series	Model	Product code	PPPoE server compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X-PWR • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	Yes

Hardware series	Model	Product code	PPPoE server compatibility
	EWPXM2WCMD0F EWPXM1MAC0F	EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	PPPoE server compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

display pppoe-server session packet

Use **display pppoe-server session packet** to display packet statistics for PPPoE sessions.

Syntax

In standalone mode:

display pppoe-server session packet [**interface** *interface-type interface-number*]

In IRF mode:

display pppoe-server session packet { **slot** *slot-number* | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about blocked users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays packet statistics for PPPoE sessions on all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display packet statistics for PPPoE sessions on VLAN-interface 1.

```
<Sysname> display pppoe-server session packet interface vlan-interface 1
Total PPPoE sessions: 2

  Ethernet interface: Vlan1                    Session ID: 1
```

```
  InPackets: 37                            OutPackets: 38
  InBytes: 390                             OutBytes: 406
  InDrops: 0                               OutDrops: 0

  Ethernet interface: Vlan1                Session ID: 2
  InPackets: 39                            OutPackets: 40
  InBytes: 340                             OutBytes: 496
  InDrops: 1                               OutDrops: 2
```

(In IRF mode.) Display packet statistics for PPPoE sessions on VLAN-interface 1.

```
<Sysname> display pppoe-server session packet interface vlan-interface 1
Total PPPoE sessions on slot 3: 1

  Ethernet interface: Vlan1                Session ID: 1
  InPackets: 40                            OutPackets: 58
  InBytes: 690                             OutBytes: 506
  InDrops: 3                               OutDrops: 1

Total PPPoE sessions on slot 4: 2

  Ethernet interface: Vlan1                Session ID: 1
  InPackets: 43                            OutPackets: 59
  InBytes: 790                             OutBytes: 576
  InDrops: 2                               OutDrops: 1

  Ethernet interface: Vlan1                Session ID: 2
  InPackets: 35                            OutPackets: 36
  InBytes: 370                             OutBytes: 386
  InDrops: 0                               OutDrops: 0
```

Table 6 Command output

Field	Description
Ethernet interface	Interface where the PPPoE session is present.
Session ID	PPPoE session ID.
InPackets	Number of packets received.
OutPackets	Number of packets transmitted.
InBytes	Number of bytes received.
OutBytes	Number of bytes transmitted.
InDrops	Number of discarded incoming packets.
OutDrops	Number of discarded outgoing packets.

Related commands

display interface virtual-access

display pppoe-server session summary

Use **display pppoe-server session summary** to display summary PPPoE session information.

Syntax

In standalone mode:

display pppoe-server session summary [**interface** *interface-type interface-number*]

In IRF mode:

display pppoe-server session summary { **slot** *slot-number* | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about blocked users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays summary PPPoE session information for all member devices. (In IRF mode.)

Usage guidelines

Summary PPPoE session information on a physical interface can be displayed only on the card where the interface resides. Summary PPPoE session information on a logical interface can be displayed on all cards.

Examples

(In standalone mode.) Display summary PPPoE session information on VLAN-interface 1.

```
<Sysname> display pppoe-server session summary interface vlan-interface 1
Total PPPoE sessions: 2

  Ethernet interface: Vlan1                Session ID: 1
  PPP interface: VA1                       State: PADR_RCVD
  Remote MAC: 00e0-1500-7100               Local MAC: 00e0-1400-7300
  Service VLAN: N/A                        Customer VLAN: N/A

  Ethernet interface: Vlan1                Session ID: 2
  PPP interface: VA2                       State: OPEN
  Remote MAC: 00e0-1500-7100               Local MAC: 00e014007400
  Service VLAN: 2                          Customer VLAN: 1
```

(In IRF mode.) Display summary PPPoE session information on VLAN-interface 1.

```
<Sysname> display pppoe-server session summary interface vlan-interface 1
Total PPPoE sessions on slot 1: 1
```

```
  Ethernet interface: Vlan1                Session ID: 1
  PPP interface: VA1                       State: PADR_RCVD
  Remote MAC: 00e0-1500-7100               Local MAC: 00e0-1400-7300
  Service VLAN: N/A                        Customer VLAN: N/A

Total PPPoE sessions on slot 2: 2

  Ethernet interface: Vlan1                Session ID: 1
  PPP interface: VA1                       State: PADR_RCVD
  Remote MAC: 00e0-1500-7100               Local MAC: 00e0-1400-7300
  Service VLAN: N/A                        Customer VLAN: N/A

  Ethernet interface: Vlan1                Session ID: 2
  PPP interface: VA2                       State: OPEN
  Remote MAC: 00e0-1500-7100               Local MAC: 00e0-1400-7400
  Service VLAN: 2                          Customer VLAN: 1
```

Table 7 Command output

Field	Description
Total PPPoE sessions	Total number of PPPoE sessions on physical interfaces and logical interfaces.
Local PPPoE sessions	Total number of PPPoE sessions on physical interfaces. When an interface is specified, this field is not displayed.
Ethernet interface	Interface where the PPPoE session is present.
Session ID	PPPoE session ID.
PPP interface	Virtual access interface created for the PPPoE session.
State	PPPoE session state: • **PADR RCVD**—The PPPoE session is being negotiated. • **Open**—The PPPoE session has been successfully established.
RemoteMAC	MAC address of the remote end.
LocalMAC	MAC address of the local end.
Service VLAN	Service provider VLAN. **N/A** means no service provider VLAN is available.
Customer VLAN	Customer VLAN. **N/A** means no customer VLAN is available.

display pppoe-server throttled-mac

Use **display pppoe-server throttled-mac** to display information about blocked users.

Syntax

In standalone mode:

display pppoe-server throttled-mac [**interface** *interface-type interface-number*]

In IRF mode:

display pppoe-server throttled-mac { **slot** *slot-number* | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about blocked users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays information about blocked users on all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display information about blocked users on VLAN-interface 1.

```
<Sysname> display pppoe-server throttled-mac interface vlan-interface 1
Total 3 client MACs:
  Interface        Remote MAC     Start time           Remaining time(s)
  Vlan1            00e0-1500-4100 2010-12-01,12:10:30  55
  Vlan1            00e0-1500-4000 2010-12-01,12:10:40  65
  Vlan1            00e0-1500-3300 2010-12-01,12:10:50  75
```

(In IRF mode.) Display information about blocked users on VLAN-interface 1.

```
<Sysname> display pppoe-server throttled-mac interface vlan-interface 1
Total 1 client MACs in slot 1:
  Interface        Remote MAC      Start time           Remaining time(s)
  Vlan1            00e0-1500-4100  2010-12-01,12:10:30  55
Total 2 client MACs in slot 2:
  Interface        Remote MAC      Start time            Remaining time(s)
  Vlan1            00e0-1500-6300  2010-12-01,12:10:30   55
  Vlan1            00e0-1500-6000  2010-12-01,12:10:40   65
  Vlan1            00e0-1500-6300  2010-12-01,12:10:50   75
```

Table 8 Command output

Field	Description
Interface	Interface at which the user is blocked.
Remote MAC	MAC address of the user.
Start time	Time to start blocking users.
Remaining time(s)	Time left for blocking users, in seconds.

Related commands

pppoe-server throttle per-mac

display pppoe-server va-pool

Use **display pppoe-server va-pool** to display information about VA pools.

Syntax

display pppoe-server va-pool

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display information about VA pools.

```
<Sysname> display pppoe-server va-pool
VT interface         Size      Unused/State
Virtual-Template1    1000      900
Virtual-Template2    1000      Creating
```

(In IRF mode.) Display information about VA pools.

```
<Sysname> display pppoe-server va-pool
Location    VT interface         Size      Unused/State
            Virtual-Template1    1000      900
0/cpu1      Virtual-Template2    1000      1000
```

Table 9 Command output

Field	Description
Location	IRF member device, card, and CPU where the VA pool resides. When the field displays a hyphen (-), it indicates a global VA pool. If the device cannot display the CPU, an asterisks (*) is displayed, for example, 1/0/*.
VT interface	Virtual-Template interface that uses the VA pool.
Unused/State	VA pool capacity available for PPP users/current state of the VA pool. • **Creating**—The VA pool is being created. • **Destroying**—The VA pool is being removed.

Related commands

pppoe-server virtual-template va-pool

ppp lcp echo mru verify

Use **ppp lcp echo mru verify** to enable maximum receive unit (MRU) verification for PPPoE on a VT interface.

Use **undo ppp lcp echo mru verify** to disable MRU verification for PPPoE.

Syntax

ppp lcp echo mru verify [**minimum** *value*]

undo ppp lcp echo mru verify

Default

MRU verification for PPPoE is disabled on a VT interface.

Views

VT interface view

Predefined user roles

network-admin

Parameters

minimum *value*: Specifies the minimum MRU in the range of 64 to 1500 bytes.

Usage guidelines

To support an MTU larger than 1492, PPPoE adds the PPP-Max-Payload option during PPPoE negotiation. This option identifies the MTU for the current PPPoE session. If the MTU is larger than 1492, PPP uses the MTU as the MRU during LCP negotiation, and reports the MTU after negotiation.

MRU verification prevents the negotiated MRU from exceeding the receiving and sending capabilities of the interface. If the negotiated MRU is larger than 1492, the PPPoE server sends an echo request that has the same size as the negotiated MRU. If the PPPoE server receives a reply, it uses the MRU as the MTU. If the PPPoE server fails to receive a reply, the following situations occur:

- If the minimum MRU is configured, the PPPoE server sends a packet that has the same size as the minimum MRU.
- If the minimum MRU is not configured, the PPPoE server sends a packet that has the same size as the negotiated MRU.

If the second verification still fails, the PPPoE server tears down the link.

NCP negotiation starts after the MRU verification succeeds.

Examples

Enable MRU verification for PPPoE and set the minimum MRU to 1200 bytes on Virtual-Template 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ppp lcp echo mru verify minimum 1200
```

pppoe-server access-delay

Use **pppoe-server access-delay** to set the response delay time on an interface.

Use **undo pppoe-server access-delay** to restore the default.

Syntax

pppoe-server access-delay *delay-time*

undo pppoe-server access-delay

Default

No response delay time is set on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the response delay time, in the range of 10 to 25500 milliseconds.

Usage guidelines

The system responds to the first packet of a PPP connection on the interface after the configured delay time elapses.

Examples

Set the response delay time to 100 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-delay 100
```

pppoe-server access-line-id bas-info

Use **pppoe-server access-line-id bas-info** to configure the NAS-Port-ID attribute to automatically include BAS information on an interface.

Use **undo pppoe-server access-line-id bas-info** to restore the default.

Syntax

pppoe-server access-line-id bas-info [**cn-163**]

undo pppoe-server access-line-id bas-info

Default

The NAS-Port-ID attribute does not automatically include BAS information on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

cn-163: Specifies the China Telecom 163 format for the BAS information. If you do not specify this keyword, BAS information in the China Telecom format is included.

Usage guidelines

he bas-info formats include China Telecom and China Telecom 163.

The China Telecom format is { eth|trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI. The format refers to the user access interface information on the BAS device, including upstream interface, VLAN, and VPI/VCI information. When Ethernet/DSL is used, XPI.XCI refers to VLAN information.

For example, eth 1/0/1:4096.2345 includes the following user access interface information:

- The type of the upstream interface is Ethernet interface.

- The interface is located at slot 1, subslot 0, and port 1.
- The outer VLAN ID is 4096 (which means an invalid VLAN), and the inner VLAN ID is 2345.

Table 10 shows the China Telecom 163 format, where:

- *NAS_slot*, *NAS_subslot*, and *NAS_port* refer to the numbering information of the PPPoE user access interface on the BAS device.
- vpi and vci refer to VPI and VCI information.
- vlanid and vlanid2 refer to inner VLAN and outer VLAN, respectively. The value for the vlanid of the primary interface is fixed at 0.

Table 10 BAS information in China Telecom 163 format

Interface type	Format
Primary interface or interface that does not carry inner VLAN or outer VLAN information.	slot=*NAS_slot*;subslot=*NAS_subslot*;port=*NAS_port*;vlanid=*VLAN id*;
Interface that carries inner VLAN and outer VLAN information.	slot=*NAS_slot*;subslot=*NAS_subslot*;port=*NAS_port*;vlanid=*VLAN id*;vlanid2=*VLAN id2*;

This command determines the content of the NAS-Port-ID attribute that the PPPoE server delivers to the RADIUS server.

- If the **cn-163** keyword is specified, the PPPoE server automatically inserts the corresponding BAS information before the parsed circuit-id. Then it sends the combination of the bas-info and circuit-id as the NAS-Port-ID attribute to the RADIUS server.
- If the **cn-163** keyword is not specified, the PPPoE server creates a new circuit-id in China Telecom format. Then it sends the new circuit-id as the NAS-Port-ID attribute to the RADIUS server. The new circuit-id contains the corresponding BAS information and the DSLAM user access information in the original circuit-id.

If this command is not executed, the NAS-Port-ID attribute that the PPPoE server delivers to the RADIUS server is determined by the **pppoe-server access-line-id content** command.

The RADIUS server cannot correctly parse a NAS-Port-ID attribute that includes the remote-id and BAS information. When you configure this command together with the **pppoe-server access-line-id trust** command, make sure the NAS-Port-ID attribute sent to the RADIUS sever does not include the remote-id.

Examples

Configure the NAS-Port-ID attribute to automatically include BAS information on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id bas-info
```

Related commands

pppoe-server access-line-id circuit-id parse-mode

pppoe-server access-line-id content

pppoe-server access-line-id trust

pppoe-server access-line-id circuit-id parse-mode

Use **pppoe-server access-line-id circuit-id parse-mode** to configure the format that an interface uses to parse the circuit-id in the access line ID.

Use **undo pppoe-server access-line-id circuit-id parse-mode** to restore the default.

Syntax

pppoe-server access-line-id circuit-id parse-mode { **cn-telecom** | **tr-101** }

undo pppoe-server access-line-id circuit-id parse-mode

Default

An interface uses the TR-101 format to parse the circuit-id.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

cn-telecom: Specifies China Telecom format.

tr-101: Specifies TR-101 format.

Usage guidelines

The circuit-id formats include TR-101 and China Telecom.

The TR-101 format is Access-Node-Identifier eth slot/port[:vlan-id] for Ethernet/DSL. The entire ID refers to the user access information on the DSLAM, where

- Access-Node-Identifier refers to the identifier of the DSLAM.
- The remainder refers to information about the user access interface on the DSLAM.

The China Telecom format is AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]. The format refers to user access information on the DSLAM, including DSLAM identifier and user access interface.

For example, the circuit-id guangzhou001/1/31/63/31/127 includes the following information:

- The identifier of the access node DSLAM is guangzhou001.
- The rack number of the DSLAM is 1.
- The user access interface is located at port 127, subslot 31, slot 63, and frame 31.

Examples

Configure GigabitEthernet 1/0/1 to use China Telecom format to parse the circuit-id.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id circuit-id parse-mode
cn-telecom
```

Related commands

pppoe-server access-line-id circuit-id trans-format

pppoe-server access-line-id circuit-id trans-format

Use **pppoe-server access-line-id circuit-id trans-format** to configure the transmission format for the circuit-id in access line ID on an interface.

Use **undo pppoe-server access-line-id circuit-id trans-format** to restore the default.

Syntax

pppoe-server access-line-id circuit-id trans-format { **ascii** | **hex** }

undo pppoe-server access-line-id circuit-id trans-format

Default

The transmission format for the circuit-id in access line ID is a string of characters on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ascii: Specifies the character string format. For example, the circuit-id 00010002 is transmitted in the form of 01 08 30 30 30 31 30 30 30 32.

hex: Specifies the hexadecimal format. For example, the circuit-id 00010002 is transmitted in the form of 01 04 00 01 00 02.

Examples

Configure GigabitEthernet 1/0/1 to use the hexadecimal format to transmit the circuit-id.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id circuit-id trans-format hex
```

pppoe-server access-line-id content

Use **pppoe-server access-line-id content** to configure the content of the NAS-Port-ID attribute delivered to the RADIUS server on an interface.

Use **undo pppoe-server access-line-id content** to restore the default.

Syntax

pppoe-server access-line-id content { **all** [*separator*] | **circuit-id** | **remote-id** }

undo pppoe-server access-line-id content

Default

The NAS-Port-ID attribute contains only the circuit-id on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

all: Sends both the circuit-id and remote-id.

separator: Specifies a separator that is one character long. By default, the value is a blank space. The circuit-id and remote-id are connected by the separator.

circuit-id: Sends only the circuit-id.

remote-id: Sends only the remote-id.

Usage guidelines

The PPPoE server on a BAS device uses the RADIUS NAS-Port-ID attribute to send the access line ID received from a DSLAM device to the RADIUS server. The access line ID contains the circuit-id and remote-id. The RADIUS server compares the received NAS-Port-ID attribute with the local line ID information to verify the location of the user.

For more information about the circuit-id, see the **pppoe-server access-line-id circuit-id parse-mode** command.

For more information about the remote-id, see **pppoe-server access-line-id remote-id trans-format** the command.

Do not use a character that exists in the circuit-id or remote-id as the separator. Otherwise, the RADIUS server might fail to parse the ID information.

This command determines the content of the NAS-Port-ID attribute only when the **pppoe-server access-line-id bas-info** command is not configured. Otherwise, the **pppoe-server access-line-id bas-info** command determines the content of the NAS-Port-ID attribute.

Examples

Configure GigabitEthernet 1/0/1 to deliver only the circuit-id to the RADIUS server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id content circuit-id
```

Related commands

pppoe-server access-line-id bas-info

pppoe-server access-line-id circuit-id parse-mode

pppoe-server access-line-id remote-id trans-format

pppoe-server access-line-id remote-id trans-format

Use **pppoe-server access-line-id remote-id trans-format** to configure the transmission format for the remote-id in the access line ID on an interface.

Use **undo pppoe-server access-line-id remote-id trans-format** to restore the default.

Syntax

pppoe-server access-line-id remote-id trans-format { **ascii** | **hex** }

undo pppoe-server access-line-id remote-id trans-format

Default

The transmission format for the remote-id is a string of characters on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ascii: Specifies the character string format.

hex: Specifies the hexadecimal format.

Usage guidelines

The remote-id is the system MAC address of a PPPoE relay device (for example, DSLAM). It can be transmitted in character strings or hexadecimal format.

Examples

Configure GigabitEthernet 1/0/1 to use the hexadecimal format to transmit the remote-id.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id remote-id trans-format hex
```

pppoe-server access-line-id trust

Use **pppoe-server access-line-id trust** to configure the PPPoE server to trust the access line ID in received packets on an interface.

Use **undo pppoe-server access-line-id trust** to restore the default.

Syntax

pppoe-server access-line-id trust

undo pppoe-server access-line-id trust

Default

The PPPoE server does not trust the access line ID in received packets on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the PPPoE server to parse the circuit-id and remote-id in a received packet, and creates a new circuit-id and remote-id. If the PPPoE server fails to parse the circuit-id or remote-id in a PADR packet, it discards the packet and does not return a PADS packet.

If this command is not executed, the PPPoE server does not parse the circuit-id and remote-id in a received packet. The contents of both the new circuit-id and the remote-id are null.

Examples

Configure GigabitEthernet 1/0/1 to trust the access line ID in received packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server access-line-id trust
```

Related commands

pppoe-server access-line-id circuit-id parse-mode

pppoe-server bind

Use **pppoe-server bind** to enable the PPPoE server on an interface and bind the interface to a VT interface.

Use **undo pppoe-server bind** to disable the PPPoE server on an interface.

Syntax

pppoe-server bind virtual-template *number*

undo pppoe-server bind

Default

The PPPoE server is disabled on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

virtual template *number*: Specifies a VT interface by its number. The value range for the number argument is 0 to 1023.

Usage guidelines

A PPPoE server-enabled interface can be bound to a nonexistent VT interface.

If the interface has been bound to a VT interface, you cannot use this command to bind the interface to another VT interface. To do that, disable the PPPoE server on the interface first.

If both the PPPoE client and PPPoE server are enabled on an interface, the PPPoE client feature does not take effect.

Examples

Enable the PPPoE server on GigabitEthernet 1/0/1 and bind the interface to Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server bind virtual-template 1
```

pppoe-server session-limit

Use **pppoe-server session-limit** to set the maximum number of PPPoE sessions on an interface.

Use **undo pppoe-server session-limit** to restore the default.

Syntax

pppoe-server session-limit *number*

undo pppoe-server session-limit

Default

The number of PPPoE sessions on an interface is not limited.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of PPPoE sessions on an interface, in the range of 1 to 65534.

Usage guidelines

PPPoE can establish a session when none of the following limits are reached:

- Limit for a user on an interface.
- Limit for a VLAN on an interface.
- Limit on an interface.
- Limit on an IRF member device. (In IRF mode.)
- Limit on a device.

New maximum number settings only apply to subsequently established PPPoE sessions.

Examples

Set the maximum number of PPPoE sessions on GigabitEthernet 1/0/1 to 50.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server session-limit 50
```

Related commands

pppoe-server session-limit per-mac

pppoe-server session-limit per-vlan

pppoe-server session-limit total

pppoe-server session-limit per-mac

Use **pppoe-server session-limit per-mac** to set the maximum number of PPPoE sessions for a user on an interface.

Use **undo pppoe-server session-limit per-mac** to restore the default.

Syntax

pppoe-server session-limit per-mac *number*

undo pppoe-server session-limit per-mac

Default

A user can create a maximum of 100 PPPoE sessions on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of PPPoE sessions for a user, in the range of 1 to 65534.

Usage guidelines

A user is identified by a MAC address.

PPPoE can establish a session when none of the following limits are reached:

- Limit for a user on an interface.
- Limit for a VLAN on an interface.
- Limit on an interface.
- Limit on an IRF member device. (In IRF mode.)
- Limit on a device.

New maximum number settings only apply to subsequently established PPPoE sessions.

Examples

Set the maximum number of PPPoE sessions for a user on GigabitEthernet 1/0/1 to 50.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server session-limit per-mac 50
```

Related commands

pppoe-server session-limit

pppoe-server session-limit per-vlan

pppoe-server session-limit total

pppoe-server session-limit per-vlan

Use **pppoe-server session-limit per-vlan** to set the maximum number of PPPoE sessions for a VLAN on an interface.

Use **undo pppoe-server session-limit per-vlan** to restore the default.

Syntax

pppoe-server session-limit per-vlan *number*

undo pppoe-server session-limit per-vlan

Default

The number of PPPoE sessions for a VLAN on an interface is not limited.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of PPPoE sessions for a VLAN, in the range of 1 to 65534.

Usage guidelines

PPPoE can establish a session when none of the following limits are reached:

- Limit for a user on an interface.
- Limit for a VLAN on an interface.

- Limit on an interface.
- Limit on an IRF member device. (In IRF mode.)
- Limit on a device.

New maximum number settings only apply to subsequently established PPPoE sessions.

Examples

Set the maximum number of PPPoE sessions for a VLAN on GigabitEthernet 1/0/1.1 to 50.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] pppoe-server session-limit per-vlan 50
```

Related commands

pppoe-server sessions limit

pppoe-server sessions limit per-mac

pppoe-server sessions limit total

pppoe-server session-limit total

Use **pppoe-server session-limit total** to set the maximum number of PPPoE sessions on a device.

Use **undo pppoe-server session-limit total** to restore the default.

Syntax

In standalone mode:

pppoe-server session-limit total *number*

undo pppoe-server session-limit total

In IRF mode:

pppoe-server session-limit slot *slot-number* **total** *number*

undo pppoe-server session-limit slot *slot-number* **total**

Default

The number of PPPoE sessions on a device is not limited. (In standalone mode.)

The number of PPPoE sessions on an IRF member device is not limited. (In IRF mode.)

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of PPPoE sessions on a device, in the range of 1 to 65534.

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Usage guidelines

PPPoE can establish a session when none of the following limits are reached:

- Limit for a user on an interface.
- Limit for a VLAN on an interface.

- Limit on an interface.
- Limit on an IRF member device. (In IRF mode.)
- Limit on a device.

The maximum number of PPPoE sessions on a device or on a card is also limited by the device specification. If the configured number is larger than the device specification, the device specification applies.

New maximum number settings only apply to subsequently established PPPoE sessions.

Examples

(In standalone mode.) Set the maximum number of PPPoE sessions on a device to 3000.

```
<Sysname> system-view
[Sysname] pppoe-server session-limit total 3000
```

(In IRF mode.) Set the maximum number of PPPoE sessions for slot 2 to 3000.

```
<Sysname> system-view
[Sysname] pppoe-server session-limit slot 2 total 3000
```

Related commands

pppoe-server session-limit

pppoe-server session-limit per-mac

pppoe-server session-limit per-vlan

pppoe-server tag ac-name

Use **pppoe-server tag ac-name** to set the access concentrator (AC) name for the PPPoE server on an interface.

Use **undo pppoe-server tag ac-name** to restore the default.

Syntax

pppoe-server tag ac-name *name*

undo pppoe-server tag ac-name

Default

The AC name for the PPPoE server is the device name on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

name: Specifies an AC name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

The PPPoE server sends its AC name in PADO packets. PPPoE clients choose a PPPoE server by AC name. The PPPoE clients on H3C devices cannot identify PPPoE servers by AC name.

The device does not support an AC name comprised of all blank spaces.

Examples

Specify the AC name for the PPPoE server on GigabitEthernet 1/0/1 as **pppoes**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server tag ac-name pppoes
```

pppoe-server tag ppp-max-payload

Use **pppoe-server tag ppp-max-payload** to enable the PPPoE server to support the ppp-max-payload tag and set a range for the tag on an interface.

Use **undo pppoe-server tag ppp-max-payload** to restore the default.

Syntax

pppoe-server tag ppp-max-payload [**minimum** *min-number* **maximum** *max-number*]

undo pppoe-server tag ppp-max-payload

Default

The PPPoE server does not support ppp-max-payload tag on an interface. The PPPoE server ignores the ppp-max-payload tag in PADI or PADS packets from clients, and returns a PADO or PADS packets without the ppp-max-payload tag.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

minimum *min-number*: Specifies the minimum value for the PPP maximum payload, in the range of 64 to 4470 bytes. The default value is 1492 bytes.

maximum *max-number*: Specifies the maximum value for the PPP maximum payload, in the range of 64 to 4470 bytes. The default value is 1500 bytes. The *max-number* argument must be equal or greater than the *min-number* argument.

Usage guidelines

This command enables the PPPoE server to forward large PPP packets with a payload larger than 1492 bytes and reduces fragmentation. If the ppp-max-payload tag sent by the PPPoE client is within the tag range, the PPPoE server returns a PADO or PADS packet that includes the tag. If not, the PPPoE server considers the received packets invalid, and it does not return a PADO or PADS packet.

The **jumboframe enable** command can change the size of jumbo frames supported by the interface. The maximum size of the jumbo frames configured by the **jumboframe enable** command should be larger than the maximum value configured by the **pppoe-server tag ppp-max-payload** command.

Examples

Enable the PPPoE server to support the ppp-max-payload tag and set the value for the PPP maximum payload to be in the range of 1494 to 1580 bytes on GigabitEthernet 1/0/1.

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

```
[Sysname-GigabitEthernet1/0/1] pppoe-server tag ppp-max-payload minimum 1494 maximum 1508
```

Related commands

jumboframe enable (*Interface Command References*)

pppoe-server tag service-name

Use **pppoe-server tag service-name** to set a service name for a PPPoE server on an interface.

Use **undo pppoe-server tag service-name** to restore the default.

Syntax

pppoe-server tag service-name *name*

undo pppoe-server tag service-name

Default

A PPPoE server does not have a service name.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

name: Specifies a service name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

Service names identify the traffic destined for PPPoE servers when multiple PPPoE servers are providing services on the network. A PPPoE client establishes a session with the target PPPoE server by using the following process:

1. The client broadcasts a PADI packet.
2. The server compares its service name with the service-name tag field of the PADI packet. The server sends a PADO packet to the client if either of the following conditions exists:
   - The field matches the service name.
   - No service name is configured.
3. The client sends a PADR packet to the server.
4. The server compares its service name with the service-name tag field of the PADR packet. The server sends a PADS packet and sets up a session with the client if either of the following conditions exists:
   - The field matches the service name.
   - No service name is configured.

Examples

Set the service name to **pppoes** for the PPPoE server on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server tag service-name pppoes
```

pppoe-server throttle per-mac

Use **pppoe-server throttle per-mac** to set the PPPoE access limit on an interface.

Use **undo pppoe-server throttle per-mac** to restore the default.

Syntax

pppoe-server throttle per-mac *session-requests session-request-period blocking-period*

undo pppoe-server throttle per-mac

Default

The PPPoE access rate is not limited on an interface.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

session-requests: Specifies the maximum number of PPPoE session requests from a user within the monitoring time. The value range is 1 to 100000.

session-request-period: Specifies the monitoring time in the range of 1 to 3600 seconds.

blocking-period: Specifies the blocking time in the range of 1 to 3600 seconds.

Usage guidelines

This command limits the rate at which a user (identified by MAC address) can create PPPoE sessions on an interface. If the number of PPPoE requests within the monitoring time exceeds the configured threshold, the device discards the excessive requests, and outputs log messages. If the blocking time is set to 0, the device does not block any requests, and it only outputs log messages.

The device uses a monitoring table and a blocking table to control PPP access rates.

- **Monitoring table**—Stores a maximum of 8000 monitoring entries. Each entry records the number of PPPoE sessions created by a user within the monitoring time. When the monitoring entries reach the maximum, the system stops monitoring and blocking session requests from new users. The aging time of monitoring entries is determined by the *session-request-period* argument. When the timer expires, the system starts a new round of monitoring for the user.
- **Blocking table**—Stores a maximum of 8000 blocking entries. The system creates a blocking entry if the access rate of a user reaches the threshold, and blocks requests from that user. When the blocking entries reach the maximum, the system stops blocking session requests from new users and it only outputs log messages. The aging time of the blocking entries is determined by the *blocking-period* argument. When the timer expires, the system starts a new round of monitoring for the user.

If the access rate setting is changed, the system removes all monitoring and blocking entries, and uses the new settings to limit PPPoE access rates.

Examples

Limit the rate at which a user can create PPPoE sessions on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-server throttle per-mac 100 100 5
```

Related commands

display pppoe-server throttled-mac

pppoe-server virtual-template va-pool

Use **pppoe-server virtual-template va-pool** to configure a VA pool.

Use **undo pppoe-server virtual-template va-pool** to remove a VA pool.

Syntax

In standalone mode:

pppoe-server virtual-template *template-number* **va-pool** *va-volume*

undo pppoe-server virtual-template *template-number* **va-pool**

In IRF mode:

pppoe-server virtual-template *template-number* [**slot** *slot-number*] **va-pool** *va-volume*

undo pppoe-server virtual-template *template-number* [**slot** *slot-number*] **va-pool**

Default

No VA pool is configured.

Views

System view

Predefined user roles

network-admin

Parameters

virtual-template *template-number*: Specifies an existing VT interface to use the VA pool.

va-pool *va-volume*: Specifies the maximum number of VA interfaces contained in the VA pool, in the range of 1 to 65534.

slot *slot-number*: Specifies an IRF member device by its IRF member ID. If you do not specify a member device, a global VA pool is created. (In IRF mode.)

Usage guidelines

The PPPoE server creates a VA interface for a PPPoE session to transmit packets between PPPoE and PPP, and removes the VA interface when the user goes offline. Creating and removing VA interfaces take time.

You can configure VA pools to improve the performance of PPPoE session establishment and termination. A VA pool contains a group of automatically numbered VA interfaces. The PPPoE server selects a VA interface from the pool for a requesting user and release the VA interface when the user goes offline. When a VA pool is exhausted, the system creates VA interfaces for new PPPoE sessions, and removes those VA interfaces when the users go offline.

On a VT interface, you can create one global VA pool and one regional VA pool per member device for interfaces bound with the VT interface.

- The global VA pool contains VA interfaces for logical interfaces that might span multiple devices, such as Ethernet aggregate interfaces.
- The regional VA pool contains VA interfaces for interfaces that do not span multiple devices, such as Ethernet interfaces.

When you configure a VA pool, follow these guidelines:

- To change the capacity of a VA pool, you must delete the previous configuration, and reconfigure the VA pool.
- Creating or removing a VA pool takes time. During the process of creating or removing a VA pool, users can go online or offline, but the VA pool does not take effect.
- If the system fails to create a VA pool because of insufficient resources, you can view the available resources by using the **display pppoe-server va-pool** command.
- VA pools are memory intensive. Set their capacity depending on your network requirements.
- Deleting a VA pool does not log off the users who are using VA interfaces in the VA pool.

Examples

Create a VA pool with a capacity of 1000 VA interfaces on Virtual-Template 2.

```
<Sysname> system-view
[Sysname] pppoe-server virtual-template 2 va-pool 1000
```

Related commands

display pppoe-server va-pool

reset pppoe-server

Use **reset pppoe-server** to clear PPPoE sessions on the PPPoE server.

Syntax

reset pppoe-server { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all PPPoE sessions.

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

virtual-template *number*: Specifies a VT interface by its number.

Examples

Clear established sessions on Virtual-template 1 on the PPPoE server.

```
<Sysname> reset pppoe-server virtual-template 1
```

PPPoE client commands

The following compatibility matrix shows the support of hardware platforms for PPPoE client:

Hardware series	Model	Product code	PPPoE client compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR	Yes

Hardware series	Model	Product code	PPPoE client compatibility
	WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X-PWR • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	PPPoE client compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No

Hardware series	Model	Product code	PPPoE client compatibility
WX5800H series	WX5860H	EWP-WX5860H-GL	No

dialer bundle enable

Use **dialer bundle enable** to enable bundle DDR on a dialer interface.

Use **undo dialer bundle enable** to disable bundle DDR on a dialer interface.

Syntax

dialer bundle enable

undo dialer bundle enable

Default

Bundle DDR is disabled on a dialer interface.

Views

Dialer interface view

Predefined user roles

network-admin

Usage guidelines

DDR includes traditional DDR and bundle DDR.

Before using bundle DDR, use this command to enable bundle DDR on a dialer interface. Then assign physical interfaces to the corresponding dialer bundle by using the **dialer bundle-member** command. To enable bundle DDR to receive calls, configure the **dialer peer-name** command on the dialer interface.

After you configure this command on a dialer interface already enabled with traditional DDR, the system clears the original traditional DDR settings.

The **undo dialer bundle enable** command clears all bundle DDR settings on the dialer interface.

Examples

Enable bundle DDR on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer bundle enable
```

dialer diagnose

Use **dialer diagnose** to configure DDR to operate in diagnostic mode.

Use **undo dialer diagnose** to restore the default.

Syntax

dialer diagnose [**interval** *interval*]

undo dialer diagnose

Default

DDR operates in non-diagnostic mode.

Views

Dialer interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the diagnostic interval in the range of 5 to 65535 seconds. The default is 120 seconds.

Usage guidelines

This command takes effect only when a dialer interface is used with PPPoE client applications.

In diagnostic mode, the device performs the following operations:

- Dials a PPPoE connection immediately after the device configurations are complete.
- Automatically terminates the connection.
- Starts the auto-dial timer after a configurable diagnostic interval.
- Redials a connection when the auto-dial timer expires.

By establishing and terminating PPPoE sessions periodically, you can monitor the operating status of the PPPoE link.

In diagnostic mode, the link idle-timeout timer is ignored.

Examples

Configure Dialer 1 to operate in diagnostic mode, with a diagnostic interval of 300 seconds.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer diagnose interval 300
```

Related commands

dialer timer autodial

dialer timer idle

dialer timer autodial

Use **dialer timer autodial** to set the auto-dial timer.

Use **undo dialer timer autodial** to restore the default.

Syntax

dialer timer autodial *autodial-interval*

undo dialer timer autodial

Default

The auto-dial timer is 300 seconds.

Views

Dialup interface view

Predefined user roles

network-admin

Parameters

autodial-interval: Specifies the interval between auto-dial attempts, in the range of 1 to 604800 seconds.

Usage guidelines

This command takes effect only when the **autodial** keyword is specified in the **dialer number** or **dialer route** command. DDR automatically dials the dial string at the specified interval until a connection is established. In the auto-dial method, dial attempts are not traffic triggered. Once a connection is established, it will not disconnect based on the idle timer mechanism.

Examples

Set the auto-dial timer to 60 seconds on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer timer autodial 60
```

dialer timer idle

Use **dialer timer idle** to set the link idle-timeout timer.

Use **undo dialer timer idle** to restore the default.

Syntax

dialer timer idle *idle* [**in** | **in-out**]

undo dialer timer idle

Default

The link idle-timeout timer is 120 seconds, and only outgoing interesting packets reset this timer.

Views

Dialup interface view

Predefined user roles

network-admin

Parameters

idle: Specifies the link idle-timeout timer value in the range of 0 to 65535 seconds.

in: Allows only incoming interesting packets to reset the timer.

in-out: Allows both incoming and outgoing interesting packets to reset the timer.

Usage guidelines

The link idle-timeout timer starts when a link is established. If no interesting packets arrive before the timer expires, DDR disconnects the link.

If you do not specify the **in** or **in-out** keyword, only outgoing interesting packets reset the timer.

If the timer is set to 0, DDR will never disconnect the link. For a PPPoE client application, if the timer is set to 0, a dialup connection is created automatically and remains active permanently.

Examples

Set the link idle-timeout timer to 50 seconds on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer timer idle 50
```

dialer-group

Use **dialer-group** to assign a dialup interface to a dialer group.

Use **undo dialer-group** to restore the default.

Syntax

dialer-group *group-number*

undo dialer-group

Default

A dialup interface does not belong to any dialer group.

Views

Dialup interface view

Predefined user roles

network-admin

Parameters

group-number: Specifies a dialer group by its number in the range of 1 to 255. Before the assignment, you must create the dialer group by using the **dialer-group rule** command.

Usage guidelines

A dialup interface can belong to only one dialer group. If you configure this command multiple times, the most recent configuration takes effect.

You must configure this command for DDR to send packets.

Examples

Assign Dialer 1 to dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule acl 3101
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer-group 1
```

Related commands

dialer-group rule

dialer-group rule

Use **dialer-group rule** to create a dialer group and configure a dial rule for it.

Use **undo dialer-group rule** to delete a dialer group.

Syntax

dialer-group *group-number* **rule** { **ip** | **ipv6** } { **deny** | **permit** | **acl** { *acl-number* | **name** *acl-name* } }

undo dialer-group *group-number* **rule** [**ip** | **ipv6**]

Default

No dialer group exists.

Views

System view

Predefined user roles

network-admin

Parameters

group-number: Specifies the number of the dialer group to be created, in the range of 1 to 255.

ip: Specifies the IPv4 protocol.

ipv6: Specifies the IPv6 protocol.

deny: Denies packets of the specified protocol.

permit: Permits packets of the specified protocol.

acl *acl-number*: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name.

Usage guidelines

A dial rule determines when an interface initiates DDR calls. You need to configure dial rules only on the initiator of DDR calls.

You can configure a dial rule to match only IP packets or use an ACL to match packets.

Permitted protocol packets or packets that match a permit statement of an ACL are interesting packets. When receiving an interesting packet, DDR performs one of the following operations:

- Sends it out and resets the idle-timeout timer if a link is present.
- Originates a new call to establish a link if no link is present.

Denied protocol packets or packets that match a deny statement of an ACL are uninteresting packets. When receiving an uninteresting packet, DDR performs one of the following operations:

- Sends it out without resetting the idle-timeout timer if a link is present.
- Drops it if no link is present.

For DDR to forward packets correctly, you must configure a dial rule and associate it with the dialup interface by using the **dialer-group** command.

Examples

Create dialer group 1 and configure DDR to place calls for IPv4 packets. Associate Dialer 1 with dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule ip permit
[Sysname] interface dialer 1
[Sysname-Dialer] dialer-group 1
```

Create dialer group 1 and configure DDR to place calls for IPv6 packets. Associate Dialer 1 with dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule ipv6 permit
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer-group 1
```

Related commands

dialer-group

display pppoe-client session packet

Use **display pppoe-client session packet** to display the protocol packet statistics for a PPPoE session.

Syntax

display pppoe-client session packet [**dial-bundle-number** *number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the *number* argument is 0 to 1023. If you do not specify this option, the command displays the protocol packet statistics for all PPPoE sessions.

Usage guidelines

To display the data packet statistics for a PPPoE session, use the **display interface virtual-access** command to display information about the specified VA interface.

Examples

Display the protocol packet statistics for all PPPoE sessions.

```
<Sysname> display pppoe-client session packet
Bundle:    1                    Interface:  GE1/0/1
InPackets: 19                   OutPackets: 19
InBytes:   816                  OutBytes:   816
InDrops:   0                    OutDrops:   0

Bundle:    2                    Interface:  GE1/0/1
InPackets: 18                   OutPackets: 18
InBytes:   730                  OutBytes:   730
InDrops:   0                    OutDrops:   0
```

Table 11 Command output

Field	Description
Bundle	Dialer bundle to which a PPPoE session belongs.
Interface	Ethernet interface where the PPPoE session is present.
InPackets	Number of packets received.
OutPackets	Number of packets transmitted.
InBytes	Number of bytes received.
OutBytes	Number of bytes transmitted.
InDrops	Number of discarded incoming packets.
OutDrops	Number of discarded outgoing packets.

Related commands

display interface virtual-access

reset pppoe-client session packet

display pppoe-client session summary

Use **display pppoe-client session summary** to display summary PPPoE session information.

Syntax

display pppoe-client session summary [**dial-bundle-number** *number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the *number* argument is 0 to 1023. If you do not specify this option, the command displays summary information for all PPPoE sessions.

Examples

Display summary information for all PPPoE sessions.

```
<Sysname> display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/1      VA0         00e0-1400-4300 00e0-1500-4100 SESSION
2      1     GE1/0/2      VA1         00e0-1500-4300 00e0-1600-4100 SESSION
```

Table 12 Command output

Field	Description
Bundle	Dialer bundle to which the PPPoE session belongs.
Interface	Ethernet interface where the PPPoE session is present.
VA	Virtual access interface created for the PPPoE session.
RemoteMAC	MAC address of the remote end.
LocalMAC	MAC address of the local end.
State	PPPoE session state: • **IDLE**—Initialization state. • **PADI SENT**—A PPPoE Active Discovery Initiation (PADI) packet has been sent, and a PPPoE Active Discovery Offer (PADO) packet is being expected. • **PADR SENT**—A PPPoE Active Discovery Request (PADR) packet has been sent, and a PPPoE Active Discovery Session-confirmation (PADS) packet is being expected. • **SESSION**—The PPPoE session has been successfully established.

mtu

Use **mtu** to set the maximum transmission unit (MTU) of a dialer interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of dialer interfaces is 1500 bytes.

Views

Dialer interface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU in bytes. The value range for this argument is 128 to 1500.

Usage guidelines

The MTU setting of a dialer interface affects the fragmentation and reassembly of IP packets.

Examples

Set the MTU of Dialer 1 to 1200 bytes.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] mtu 1200
```

pppoe-client

Use **pppoe-client** to establish a PPPoE session and specify the dialer bundle corresponding to the session.

Use **undo pppoe-client** to remove a PPPoE session.

Syntax

pppoe-client dial-bundle-number *number* [**no-hostuniq**]

undo pppoe-client dial-bundle-number *number*

Default

No PPPoE session is established.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. A dialer bundle number uniquely identifies a PPPoE session. It can also be used as a PPPoE session ID. The value range for the *number* argument is 0 to 1023.

no-hostuniq: Configures the client not to carry the Host-Uniq field in discovery packets. If you do not specify this keyword, the client carries the Host-Unique field. The Host-Unique field uniquely identifies a PPPoE client when an interface is configured with multiple PPPoE sessions. When the PPPoE server receives a packet with this field, it must include this field unmodified in the response packet. The device identifies the PPPoE client where the response packet belongs based on the Host-Unique field in the response packet.

Examples

Establish a PPPoE session on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-client dial-bundle-number 1
```

Establish a PPPoE session on VLAN-Interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] pppoe-client dial-bundle-number 1
```

reset pppoe-client

Use **reset pppoe-client** to reset a PPPoE session corresponding to a dialer bundle.

Syntax

reset pppoe-client { **all** | **dial-bundle-number** *number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Resets all the PPPoE sessions.

dial-bundle-number *number*: Specifies a dialer bundle by its number. The value range for the *number* argument is 0 to 1023.

Usage guidelines

A PPPoE session in permanent mode and terminated by this command will be established again when the auto dial timer expires.

A PPPoE session in on-demand mode and terminated by this command will be established again only when there is a need for data transmission.

Examples

Reset all PPPoE sessions.

```
<Sysname> reset pppoe-client all
```

Related commands

dialer timer autodial

reset pppoe-client session packet

Use **reset pppoe-client session packet** to reset the protocol packet statistics for a PPPoE session.

Syntax

reset pppoe-client session packet [**dial-bundle-number** *number*]

Views

User view

Predefined user roles

network-admin

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the *number* argument is 0 to 1023. If you do not specify this option, the command resets the protocol packet statistics for all PPPoE sessions.

Examples

Reset the protocol packet statistics for all PPPoE sessions.

```
<Sysname> reset pppoe-client session packet
```

Related commands

display pppoe-client session packet

Contents

L2TP commands 1

allow l2tp 2
display l2tp session 3
display l2tp session temporary 4
display l2tp tunnel 5
display l2tp va-pool 6
display ppp access-control interface 7
ip dscp 8
l2tp enable 9
l2tp icrq-limit 9
l2tp tsa-id 10
l2tp virtual-template va-pool 11
l2tp-group 12
mandatory-chap 13
mandatory-lcp 14
ppp access-control enable 15
reset l2tp tunnel 16
tunnel authentication 16
tunnel flow-control 17
tunnel name 18
tunnel password 19
tunnel timer hello 20
tunnel window receive 20
tunnel window send 22

L2TP commands

The following compatibility matrixes show the support of hardware platforms for L2TP:

Hardware series	Models	Product code	L2TP compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X-PWR • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	Yes

Hardware series	Models	Product code	L2TP compatibility
	EWPXM1MAC0F	EWPXM1MAC0F	

Hardware series	Models	Product code	L2TP compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

allow l2tp

Use **allow l2tp** to configure an L2TP network server (LNS) to accept Layer 2 Tunneling Protocol (L2TP) tunneling requests from an L2TP access concentrator (LAC), and to specify a VT interface for tunnel setup.

Use **undo allow** to restore the default.

Syntax

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name*]

undo allow

Default

An LNS denies L2TP tunneling requests from any LACs.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

virtual-template *virtual-template-number*: Specifies a VT interface by its number. The value range for the *virtual-template-number* argument is 0 to 1023.An LNS dynamically creates virtual access (VA) interfaces based on the configuration of a VT interface. Each VA interface is used to carry data for a different L2TP session.

remote *remote-name*: Specifies the name of the tunnel peer (LAC) initiating tunneling requests, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **allow l2tp** command is available only on L2TP groups in LNS mode.

Make sure the specified name of the tunnel peer is consistent with the local name configured on the LAC.

If you execute this command multiple times for an L2TP group, the most recent configuration takes effect.

For L2TP group 1, if you do not specify the **remote** *remote-name* option, an LNS accepts tunneling requests from any LACs. In this case, L2TP group 1 acts as the default L2TP group. For L2TP groups other than L2TP group 1, the **remote** *remote-name* option must be configured.

The **allow l2tp** command is available only on LNSs.

- When an LAC that initiates a tunneling request is the tunnel peer configured in an L2TP group, the LNS uses the tunnel parameters configured in this group for tunnel setup.
- When the LAC is not the tunnel peer configured in any L2TP group, the LNS performs one of the following operations:
  - Uses the tunnel parameters for the default L2TP group if it exists.
  - Fails to set up a tunnel with the LAC if the default L2TP group does not exist.

As a best practice, configure a default L2TP group on the LNS in the following cases:

- LACs (such as hosts with Windows 2000 Beta 2 installed) include blank local names in their tunneling requests.
- The LNS sets up tunnels with multiple LACs by using the same tunnel parameters.

Examples

Specify L2TP group 1 as the default L2TP group, and specify Virtual-Template 1 for tunnel setup. For L2TP group 2, configure the LNS to accept the L2TP tunneling request initiated by the peer (LAC) named **aaa**, and specify Virtual-Template 2 for tunnel setup.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] allow l2tp virtual-template 1
[Sysname-l2tp1] quit
[Sysname] l2tp-group 2 mode lns
[Sysname-l2tp2] allow l2tp virtual-template 2 remote aaa
```

Related commands

tunnel name

display l2tp session

Use **display l2tp session** to display information about L2TP sessions.

Syntax

display l2tp session [**statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`statistics`: Displays statistics for L2TP sessions.

Examples

Display statistics for L2TP sessions.

```
<Sysname> display l2tp session statistics
Total number of sessions: 1
```

Display information about L2TP sessions.

```
<Sysname> display l2tp session
LocalSID      RemoteSID      LocalTID      State
89            36245          10878         Established
```

Table 1 Command output

Field	Description
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
State	Session state: • **Idle**. • **Wait-tunnel**—Waits for the tunnel to be established. • **Wait-reply**—Waits for an Incoming-Call-Reply (ICRP) message indicating the call is accepted. • **Wait-connect**—Waits for an Incoming-Call-Connected (ICCN) message. • **Established**.

display l2tp session temporary

Use **`display l2tp session temporary`** to display information about temporary L2TP sessions.

Syntax

`display l2tp session temporary`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about temporary L2TP sessions.

```
<Sysname> display l2tp session temporary
Total number of temporary sessions: 6
LocalSID    RemoteSID    LocalTID    State
2298        0            19699       Wait-tunnel
42805       0            19699       Wait-tunnel
17777       0            19699       Wait-tunnel
58284       0            19699       Wait-tunnel
33256       0            19699       Wait-tunnel
8228        0            19699       Wait-tunnel
```

Table 2 Command output

Field	Description
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
State	Session state: • **Idle**. • **Wait-tunnel**—Waits for the tunnel to be established. • **Wait-reply**—Waits for an ICRP message indicating the call is accepted. • **Wait-connect**—Waits for an ICCN message.

display l2tp tunnel

Use **display l2tp tunnel** to display information about L2TP tunnels.

Syntax

display l2tp tunnel [**statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

statistics: Displays statistics for L2TP tunnels.

Examples

Display statistics for L2TP tunnels.

```
<Sysname> display l2tp tunnel statistics
Total number of tunnels: 1
```

Display information about L2TP tunnels.

```
<Sysname> display l2tp tunnel
LocalTID RemoteTID State         Sessions RemoteAddress    RemotePort RemoteName
10878    21        Established   1        20.1.1.2         1701       lns
```

Table 3 Command output

Field	Description
LocalTID	Local tunnel ID.
RemoteTID	Remote tunnel ID.
State	Tunnel state: • **Idle**. • **Wait-reply**. • **Wait-connect**. • **Established**. • **Stopping**.
Sessions	Number of sessions within the tunnel.
RemoteAddress	IP address of the peer.
RemotePort	UDP port number of the peer.
RemoteName	Name of the tunnel peer.

Related commands

`reset l2tp tunnel`

display l2tp va-pool

Use **`display l2tp va-pool`** to display information about L2TP VA pools.

Syntax

`display l2tp va-pool`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about L2TP VA pools.

```
<Sysname> display l2tp va-pool
VT interface          Size      Unused      State
Virtual-Template1     1000      900         Normal
```

Table 4 Command output

Field	Description
VT interface	VT interface that uses the VA pool.
Size	VA pool capacity set for L2TP users.
Unused	VA pool capacity available for L2TP users.
State	Current state of the VA pool: • **Creating**—The VA pool is being created. • **Destroying**—The VA pool is being removed. • **Normal**—The VA pool has been created.

Related commands

`l2tp virtual-template va-pool`

display ppp access-control interface

Use **`display ppp access-control interface`** to display access control information for PPP sessions on a VT interface.

Syntax

`display ppp access-control interface virtual-template` *`interface-number`*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`virtual-template` *`interface-number`*: Specifies an existing VT interface by its number.

Examples

Display access control information for PPP sessions on Virtual-Template 2.

```
<Sysname> display ppp access-control interface virtual-template 2
Interface: Virtual-Template2:0
  User Name: mike
  In-bound Policy: acl 3000
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.

  Interface: Virtual-Template2:1
  User Name: tim
  In-bound Policy: acl 3001
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

Table 5 Command output

Field	Description
Interface	BAS interface that the PPP user accesses.
User Name	Username of the PPP user.
In-bound Policy	Security ACLs for the PPP user.
Totally x packets, x bytes, x% permitted	Total number, data rate, and pass percentage of permitted packets.
Totally x packets, x bytes, x% denied	Total number, data rate, and reject percentage of denied packets.

Related commands

ppp access-control enable

ip dscp

Use **ip dscp** to set the DSCP value of L2TP packets.

Use **undo ip dscp** to restore the default.

Syntax

ip dscp *dscp-value*

undo ip dscp

Default

The DSCP value of L2TP packets is 0.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value of L2TP packets, in the range of 0 to 63.

Usage guidelines

The DSCP field is the IP ToS byte. This field marks the priority of IP packets for forwarding. This command sets the DSCP value for the IP packet when L2TP encapsulates a PPP frame into an IP packet.

Examples

Set the DSCP value of L2TP packets to 50.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] ip dscp 50
```

l2tp enable

Use **l2tp enable** to enable L2TP.

Use **undo l2tp enable** to disable L2TP.

Syntax

l2tp enable

undo l2tp enable

Default

L2TP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For L2TP configurations to take effect, you must enable L2TP.

Examples

Enable L2TP.

```
<Sysname> system-view
[Sysname] l2tp enable
```

l2tp icrq-limit

Use **l2tp icrq-limit** to set the maximum number of incoming call request (ICRQ) packets that the LNS can process per second.

Use **undo l2tp icrq-limit** to restore the default.

Syntax

l2tp icrq-limit *number*

undo l2tp icrq-limit

Default

The maximum number of ICRQ packets that the LNS can process per second is not limited.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the ICRQ packet processing limit in the range of 1 to 1000.

Usage guidelines

To avoid device performance degradation and make sure the LNS can process ICRQ requests correctly, use this command to adjust the ICRQ packet processing rate limit.

Examples

Set the maximum number of ICRQ packets that the LNS can process per second to 200.

```
<Sysname> system-view
[Sysname] l2tp icrq-limit 200
```

l2tp tsa-id

Use **l2tp tsa-id** to set the TSA ID for the L2TP tunnel switching (LTS) device and enable L2TP loop detection on the LTS device.

Use **undo l2tp tsa-id** to restore the default.

Syntax

l2tp tsa-id *tsa-id*

undo l2tp tsa-id

Default

The TSA ID of the LTS device is not set, and L2TP loop detection is disabled on the LTS device.

Views

System view

Predefined user roles

network-admin

Parameters

tsa-id: Specifies a TSA ID that uniquely identifies the LTS device. This argument is a case-sensitive string of 1 to 64 characters.

Usage guidelines

The LTS device compares the configured TSA ID with each TSA ID Attribute Value Pair (AVP) in a received ICRQ packet for loop detection.

- If a match is found, a loop exists. The LTS immediately tears down the session.
- If no match is found, the LTS performs the following operations:
  a. Encapsulates the configured TSA ID into a new TSA ID AVP.
  b. Appends the new TSA ID AVP to the packet.
  c. Sends the packet to the next hop LTS.

To avoid loop detection errors, make sure the TSA ID of each LTS device is unique.

Examples

Set the TSA ID of the LTS device to **lts0**, and enable L2TP loop detection on the LTS device.

```
<Sysname> system-view
[Sysname] l2tp tsa-id lts0
```

l2tp virtual-template va-pool

Use **l2tp virtual-template va-pool** to create a VA pool.

Use **undo l2tp virtual-template va-pool** to delete a VA pool.

Syntax

l2tp virtual-template *template-number* **va-pool** *va-volume*

undo l2tp virtual-template *template-number* **va-pool**

Default

No VA pool exists.

Views

System view

Predefined user roles

network-admin

Parameters

virtual-template *template-number*: Specifies an existing VT interface by its number to use the VA pool.

va-pool *va-volume*: Specifies the maximum number of VA interfaces contained in the VA pool, in the range of 1 to 65534.

Usage guidelines

The LNS creates a VA interface for an L2TP session to exchange packets with the LAC, and it deletes the VA interface when the user goes offline. Creating and deleting VA interfaces take time. If a large number of users are coming online or going offline, the performance of L2TP connection establishment and termination will be degraded.

You can configure a VA pool to improve the performance. A VA pool contains a group of VA interfaces. The LNS selects a VA interface from the pool for a requesting user and places the interface back to the VA pool when the user goes offline. This mechanism speeds up the establishment and termination of L2TP connections. When a VA pool is exhausted, the system still creates a VA interface for an L2TP connection and deletes it when the user goes offline.

When you configure a VA pool, follow these guidelines:

- A VT interface can be associated with only one VA pool. To change the capacity of a VA pool, delete the previous configuration, and reconfigure the VA pool.

- Creating or deleting a VA pool takes time. During the process of creating or deleting a VA pool, users can come online or go offline, but the VA pool does not take effect.
- The system might create a VA pool that contains VA interfaces less than the specified number because of insufficient resources. In this case, you can use the **display l2tp va-pool** command to view the number of available VA interfaces and current state of the VA pool.
- Create a VA pool with an appropriate capacity, because a VA pool occupies much system memory.
- Deleting a VA pool does not log off the users who are using VA interfaces in the VA pool.

Examples

Create a VA pool with a capacity of 1000 VA interfaces for Virtual-template 2.

```
<Sysname> system-view
[Sysname] l2tp virtual-template 2 va-pool 1000
```

Related commands

display l2tp va-pool

l2tp-group

Use **l2tp-group** to create an L2TP group and enter its view, or enter the view of an existing L2TP group.

Use **undo l2tp-group** to delete an L2TP group.

Syntax

l2tp-group *group-number* [**mode** { **lac** | **lns** }]

undo l2tp-group *group-number*

Default

No L2TP group exists.

Views

System view

Predefined user roles

network-admin

Parameters

group-number: Specifies an L2TP group by its number in the range of 1 to 65535.

mode: Specifies a mode for the L2TP group.

lac: Specifies the LAC mode.

lns: Specifies the LNS mode.

Usage guidelines

To create a new L2TP group, you must specify the **mode** keyword. To enter the view of an existing L2TP group, you do not need to specify this keyword.

In L2TP group view, you can configure L2TP tunnel parameters, such as tunnel authentication and flow control.

A device can have L2TP groups in both LAC and LNS modes at the same time.

Examples

Create L2TP group 2 in LAC mode, and enter its view.

```
<Sysname> system-view
[Sysname] l2tp-group 2 mode lac
[Sysname-l2tp2]
```

Related commands

allow l2tp

lns-ip

user

mandatory-chap

Use **mandatory-chap** to force the LNS to perform CHAP authentication for users.

Use **undo mandatory-chap** to restore the default.

Syntax

mandatory-chap

undo mandatory-chap

Default

An LNS does not perform CHAP authentication for users.

Views

L2TP group view

Predefined user roles

network-admin

Usage guidelines

The LNS uses the LAC as an authentication proxy. The LAC sends the LNS all user authentication information from users and the authentication method configured on the LAC itself. The LNS then checks the user validity according to the received information and the locally configured authentication method.

When mandatory CHAP authentication is configured, a user who depends on an LAC to initiate tunneling requests is authenticated by both the LAC and the LNS for increased security. Some users

might not support the authentication on the LNS. In this situation, do not configure this command, because CHAP authentication on the LNS will fail.

This command is available only on L2TP groups in LNS mode.

This command takes effect only on NAS-initiated L2TP tunnels.

The **mandatory-lcp** command takes precedence over this command. If both commands are configured for an L2TP group, the LNS performs LCP renegotiation with the user.

Examples

Force the LNS to perform CHAP authentication for users.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] mandatory-chap
```

Related commands

mandatory-lcp

mandatory-lcp

Use **mandatory-lcp** to force an LNS to perform LCP negotiation with users.

Use **undo mandatory-lcp** to restore the default.

Syntax

mandatory-lcp

undo mandatory-lcp

Default

An LNS does not perform LCP negotiation with users.

Views

L2TP group view

Predefined user roles

network-admin

Usage guidelines

By default, to establish a NAS-initiated tunnel, the user performs LCP negotiation with the LAC. If the negotiation succeeds, the LAC initiates a tunneling request and sends the negotiation results (including authentication information) to the LNS. Then, the LNS determines whether the user is valid based on the information received instead of performing LCP renegotiation with the user.

If you do not expect the LNS to accept LCP negotiation parameters, configure this command to perform an LCP negotiation between the LNS and the user. In this case, the information sent by the LAC will be ignored.

Some users might not support LCP negotiation. In this case, do not configure this command because LCP negotiation will fail.

This command is available only on L2TP groups in LNS mode.

This command takes effect only on NAS-initiated L2TP tunnels.

This command takes precedence over the **mandatory-chap** command. If both commands are configured for an L2TP group, the LNS performs LCP negotiation with the user.

Examples

Force an LNS to perform LCP negotiation with users.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] mandatory-lcp
```

Related commands

mandatory-chap

ppp access-control enable

Use **ppp access-control enable** to enable L2TP-based EAD.

Use **undo ppp access-control enable** to disable L2TP-based EAD.

Syntax

ppp access-control enable

undo ppp access-control enable

Default

L2TP-based EAD is disabled.

Views

VT interface view

Predefined user roles

network-admin

Usage guidelines

This command does not apply to PPP sessions that already exist on the VT interface. It only applies to newly created PPP sessions on the VT interface.

Different ACLs can be used for different users if the VT interface is used as the access interface for the LNS.

L2TP-based EAD enables the LNS to transparently pass CAMS/IMC packets to the iNode client to inform the client of EAD server information, such as the IP address.

Examples

Enable L2TP-based EAD.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ppp access-control enable
```

Related commands

display ppp access-control interface

reset l2tp tunnel

Use **reset l2tp tunnel** to disconnect tunnels and all sessions within the tunnels.

Syntax

reset l2tp tunnel { **id** *tunnel-id* | **name** *remote-name* }

Views

User view

Predefined user roles

network-admin

Parameters

id *tunnel-id*: Specifies a tunnel by its local ID in the range of 1 to 65535.

name *remote-name*: Specifies L2TP tunnels by the tunnel peer name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When the number of user connections is 0 or a network fault occurs, you can disconnect the L2TP tunnel by using this command on either the LAC or LNS. After the tunnel is disconnected, all sessions within it are disconnected.

If you specify a tunnel peer name, all tunnels with the tunnel peer name will be disconnected. If no tunnel with the tunnel peer name exists, nothing happens.

A tunnel disconnected by force can be re-established when a client makes a call.

Examples

Disconnect all tunnels with the tunnel peer name of **aaa**.

```
<Sysname> reset l2tp tunnel name aaa
```

Related commands

display l2tp tunnel

tunnel authentication

Use **tunnel authentication** to enable L2TP tunnel authentication.

Use **undo tunnel authentication** to disable L2TP tunnel authentication.

Syntax

tunnel authentication

undo tunnel authentication

Default

L2TP tunnel authentication is enabled.

Views

L2TP group view

Predefined user roles

network-admin

Usage guidelines

Tunnel authentication prevents the local end from establishing L2TP tunnels with illegal remote ends.

You can enable tunnel authentication on both sides or either side.

To ensure a successful tunnel establishment when tunnel authentication is enabled on both sides or either side, set the same non-null key on the LAC and the LNS. To set the tunnel authentication key, use the **tunnel password** command.

When neither side is enabled with tunnel authentication, the key settings of the LAC and the LNS do not affect the tunnel establishment.

For tunnel security, enable tunnel authentication.

Examples

Enable L2TP tunnel authentication.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] tunnel authentication
```

Related commands

tunnel password

tunnel flow-control

Use **tunnel flow-control** to enable L2TP session flow control.

Use **undo tunnel flow-control** to disable L2TP session flow control.

Syntax

tunnel flow-control

undo tunnel flow-control

Default

L2TP session flow control is disabled.

Views

L2TP group view

Predefined user roles

network-admin

Usage guidelines

This feature adds sequence numbers to transmitted packets and uses them to reorder packets arriving out of order and to detect lost packets.

This feature takes effect on both sent and received L2TP data messages. The L2TP sessions support this feature if either the LAC or LNS is enabled with this feature.

When the device acts as an LAC, a change in the flow control status on the LNS causes the same change in the flow control status of L2TP sessions. When the device acts as an LNS, a change in the flow control status on the LAC does not affect the flow control status of L2TP sessions.

Examples

Enable L2TP session flow control.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel flow-control
```

tunnel name

Use **tunnel name** to specify the local tunnel name.

Use **undo tunnel name** to restore the default.

Syntax

tunnel name *name*

undo tunnel name

Default

The local tunnel name is the device name. For more information about the device name, see *System Management Configuration Guide*.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

name: Specifies the local tunnel name, a case-sensitive string of 1 to 31 characters.

Examples

Specify the local tunnel name as **itsme**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] tunnel name itsme
```

Related commands

sysname (*Fundamentals Command Reference*)

tunnel password

Use **tunnel password** to configure the key for tunnel authentication.

Use **undo tunnel password** to restore the default.

Syntax

tunnel password { **cipher** | **simple** } *string*

undo tunnel password

Default

No key is configured for tunnel authentication.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters.

Usage guidelines

For this command to take effect, you must enable tunnel authentication by using the **tunnel authentication** command.

For the tunnel authentication key change to take effect, change the tunnel authentication key before tunnel negotiation is performed.

Examples

Configure the key for tunnel authentication to a plaintext key **yougotit**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel password simple yougotit
```

Related commands

tunnel authentication

tunnel timer hello

Use **tunnel timer hello** to set the Hello interval.

Use **undo tunnel timer hello** to restore the default.

Syntax

tunnel timer hello *hello-interval*

undo tunnel timer hello

Default

The Hello interval is 60 seconds.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

hello-interval: Specifies the interval at which the LAC or the LNS sends Hello packets, in the range of 60 to 1000 seconds.

Usage guidelines

The device sends Hello packets at the set interval. This prevents the L2TP tunnels and sessions from being removed due to timeouts.

You can set different Hello intervals for the LNS and LAC.

Examples

Set the Hello interval to 90 seconds.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel timer hello 90
```

tunnel window receive

Use **tunnel window receive** to set the receiving window size for an L2TP tunnel.

Use **undo tunnel window receive** to restore the default.

Syntax

tunnel window receive *size*

undo tunnel window receive

Default

The receiving window size for an L2TP tunnel is 1024.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

size: Specifies the receiving window size in the range of 1 to 5000. It is the number of packets that can be buffered at the local end.

Usage guidelines

To enable the device to process a larger number of disordered packets, use this command to enlarge the receiving window size for an L2TP tunnel.

The device uses a receiving window to reorder disordered packets based on packet sequence numbers.

If the sequence number of a packet is within the receiving window but does not equal the minimum value of the window, the device performs the following operations:

1. The device buffers the packet.
2. The minimum value and maximum value of the receiving window increment by one.
3. The device continues to check the next arriving packet.

If the sequence number of a packet equals the minimum value of the receiving window, the device performs the following operations:

1. The device processes the packet.
2. The minimum value and maximum value of the receiving window increment by one.
3. The device checks buffered packets for a packet with the sequence number equal to the new minimum value of the receiving window.
4. If no required packet is found, the device checks the next arriving packet.

If the sequence number of a packet is not within the receiving window, the device drops the packet.

In the L2TP tunnel establishment process, the device uses the value specified in L2TP group view as the receiving window size.

Changing the receiving window size after an L2TP tunnel is established does not affect the established L2TP tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the receiving window size for L2TP group 1 to 128.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel window receive 128
```

Related commands

tunnel window send

tunnel window send

Use **tunnel window send** to set the sending window size for an L2TP tunnel.

Use **undo tunnel window send** to restore the default.

Syntax

tunnel window send *size*

undo tunnel window send

Default

The sending window size for an L2TP tunnel is 0, which means using the value of the receiving window size carried in messages sent by the peer end in the tunnel establishment process.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

size: Specifies the sending window size for an L2TP tunnel, in the range of 0 to 1024. It is the maximum number of packets the device can send to a peer end when the device receives no response from the peer end. If the messages from the peer end carry no receiving window size in the tunnel establishment process, the sending window size for the device is 4.

Usage guidelines

The packet processing capability of a peer end might mismatch the receiving window size of the peer end in some networks. For example, the actual packet processing capability of the peer end is 10, but the receiving window size of the peer end is 20. To ensure stable L2TP services, you can adjust the sending window size for the device to match the actual packet processing capability of the peer end.

The sending window size set in L2TP group view is obtained in the L2TP tunnel establishment process.

- If the sending window size is 0, the device uses the default sending window size.
- If the sending window size is not 0, the device uses the specified value as the sending window size.

Changing the sending window size after an L2TP tunnel is established does not affect the established L2TP tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the sending window size for L2TP group 1 to 128.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel window send 128
```

Related commands

tunnel window receive

Contents

Modem management commands 1
modem callback 2
sendat 2

Modem management commands

The following compatibility matrixes show the support of hardware platforms for modem management:

Hardware series	Model	Product code	Modem management compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	No
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: EWP-WX2508H-PWR-LTE No: • EWP-WX2510H-PWR • EWP-WX2510H-F-PWR • EWP-WX2540H • EWP-WX2540H-F • EWP-WX2560H
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Modem management compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	No
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

modem callback

Use **modem callback** to enable callback.

Use **undo modem callback** to disable callback.

Syntax

modem callback

undo modem callback

Default

Callback is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The callback function enables a modem to disconnect an incoming call and call back the calling party upon request.

Examples

Enable the callback function.

```
<Sysname> system-view
[Sysname] modem callback
```

sendat

Use **sendat** to issue an AT command to a modem.

Syntax

sendat *at-string*

Views

Interface view

Predefined user roles

network-admin

Parameters

at-string: Specifies an AT command, a case-insensitive string of 1 to 300 characters. The router automatically converts lowercase characters to uppercase when it sends the command to the modem. Enter the **AT** prefix before all commands except **A/** (Repeat Last Command) and **+++** (Escape code). For more information about AT commands that begin with **AT**, see Table 1.

Usage guidelines

CAUTION:

This command changes the modem operating state. Incorrect use of this command can cause issues such as dial-up failure. When you use this command, make sure you understand the impact of this command.

To send AT commands to a modem, you must first place the modem in AT command mode. To confirm that you can send AT commands, enter **sendat at**. The modem will return **OK** or **0** if it is ready to accept AT commands.

One **sendat** command can issue one AT command. To send multiple AT commands to a modem, you must repeat the **sendat** command.

This command does not verify the validity of AT commands. To verify the AT command execution result, enable modem debugging on the interface. To view the AT commands sent to the modem, issue the **E1** command to the modem.

Table 1 describes commonly used AT commands. Support for AT commands varies by modems.

Table 1 AT commands in common use

Command	Description
A	Forces the modem to go off-hook in answer mode. If a call is coming in, the modem will try to answer it without waiting for the ringtone. This command is useful when manual answer mode is used.
B*n*	Sets the modulation protocol preference. Available options: • **B0**—Selects the ITU V.22 mode. The transmission speed is 1200 bps. • **B1**—Selects the Bell 212 mode. The default transmission speed is 1200 bps. • **B2**/**B3**—Cancels the ITU V.23 backward channel. • **B15**—Selects the ITU V.21 mode. The transmission speed is 300 bps. • **B16**—Selects the 103J mode. The transmission speed is 300 bps. This setting is the default for Compaq Presario 192-VS and Compaq Presario 288-VS modems.
D*n*	Dials a telephone number. The *n* argument represents the dial string. In pulse dialing mode, the modem ignores nonnumeric characters.
E*n*	Controls echo of commands to the configuration terminal. Available options: • **E0**—Disables echo of commands to the configuration terminal. • **E1**—Enables echo of commands to the configuration terminal. This option is the default.
H*n*	Sets the method to terminate a call. Available options: • **H0**—Forces modem on-hook to hang up the line (the default). • **H1**—Forces modem off-hook to answer or dial.
I*n*	Displays modem information and results of checksum tests on firmware. Available options: • **I0/I3**—Displays the default transmission speed and controller firmware version.

Command	Description
	• **I1**—Runs a checksum on the ROM and displays the result. • **I2**—Runs a checksum on the ROM and displays the checksum status: ○ **OK**—The checksum is correct. ○ **ERROR**—The checksum is incorrect. • **I4**—Displays the hardware version of the data pump. • **I5**—Displays the product code, software version, hardware version, and country code. • **I9**—Displays the country code.
L*n*	Sets the speaker loudness for fax and data communication. Available options: • **L0/L1**—Low volume. • **L2**—Medium volume (the default). • **L3**—High volume.
M*n*	Sets the speaker mode for fax and data communication. Available options: • **M0**—Speaker is always off. • **M1**—Speaker is on until the carrier is detected. This option is the default. • **M2**—Speaker is on when the modem is off-hook. • **M3**—Speaker is on after a dial until the carrier is detected.
N*n*	Sets the modulation negotiation mode for the modem to establish a connection with a remote modem operating at a different speed. Available options: • **N0**—Forces the modem to connect at the speed specified in the S37 register and the **ATB***n* command. • **N1**—Enables the modem to start connecting at the speed specified in the S37 register and **ATB***n* command. However, the speed may drop during the negotiation. This option is the default.
O*n*	Forces the modem to return to data mode. Available options: • **O0**—Returns to data mode. • **O1**—Initiates an equalizer retrain sequence before returning to data mode. • **O3**—Negotiates the transmission speed before returning to data mode. After you use the **+++** command to place the command in command mode, you can use an **ATO***n* command to change the modem to data mode.
Q*n*	Enables or disables the modem to send result and status codes to the configuration terminal. Available options: • **Q0**—The modem sends result and status codes. This option is the default. • **Q1**—The modem does not send result and status codes.
S*r***=***n*	Sets the contents of S register *r* to value *n*. • **Value range for the *r* argument**—0 to 27, 29, 31 to 33, 35, 37, and 89. • **Value range for the *n* argument**—0 to 255.
T	Sets tone dialing (the default). This command can also be used as a dialing modifier.
P	Sets pulse dialing. After you execute this command, the modem performs pulse dialing for all calls until you execute the **T** command. The **P** command can also be used as a dialing modifier.
V*n*	Specifies the result code format.

Command	Description
	Available options: • **V0**—Sends numeric result codes. • **V1**—Sends text-form result codes (the default).

Contents

4G modem management commands 1

Common management commands 2
controller cellular 2
description 2
display cellular 3
display controller cellular 7
modem reboot 8
reset counters controller cellular 9
sendat 9
shutdown 10
sim switch-to 11
4G modem-specific management commands 12
apn-profile 12
bandwidth 12
default 13
description 13
display interface eth-channel 14
eth-channel 17
interface eth-channel 18
mtu 18
reset counters interface 19
shutdown 19

4G modem management commands

The following compatibility matrixes show the support of hardware platforms for 3G/4G modem management:

Hardware series	Model	Product code	3G/4G modem management compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	No
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: EWP-WX2508H-PWR-LTE No: • EWP-WX2510H-PWR • EWP-WX2510H-F-PWR • EWP-WX2540H • EWP-WX2540H-F • EWP-WX2560H
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	No

Hardware series	Model	Product code	3G/4G modem management compatibility
	EWPXM1MAC0F	EWPXM1MAC0F	

Hardware series	Model	Product code	3G/4G modem management compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	No
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Common management commands

controller cellular

Use **controller cellular** to enter cellular interface view.

Syntax

controller cellular *cellular-number*

Views

System view

Predefined user roles

network-admin

Parameters

cellular-number: Specifies a cellular interface by its number.

Examples

Enter Cellular 1/0/6 interface view.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular 1/0/6]
```

description

Use **description** to configure a description for a cellular interface.

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

Syntax

description *text*

undo description

Default

The description for a cellular interface is in the *interface name* **Interface** format, for example, Cellular 1/0/6 Interface.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

text: Sets an interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description for Cellular 1/0/6 to **Cellular-intf**.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] description Cellular-intf
```

display cellular

Use **display cellular** to display call connection information for a 4G modem.

Syntax

display cellular [*interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

cellular [*interface-number*]: Specifies a cellular interface by its number. If you do not specify a cellular interface, this command displays call connection information for all cellular interfaces with 4G modems installed.

Usage guidelines

The command output might vary by modem manufacturers.

Examples

Display call connection information for a 4G modem (LTE network).

```
<Sysname> display cellular 1/0/6
Cellular1/0/6:
  Hardware Information:
    Model: U9300C SXNC
    Manufacturer: LONGSUNG
    Modem Firmware Version: 30027
    Hardware Version:-Part=290  version=1
    International Mobile Subscriber Identity (IMSI): None
    International Mobile Equipment Identity (IMEI): 863284043221643
    Modem Status: Online
```

```
Profile Information:
  Profile index: 1
    PDP Type: IPv4
    Header Compression: Off
    Data Compression: Off
    Access Point Name (APN): wonet
  Profile index: 2
    PDP Type: IPv4
    Header Compression: Off
    Data Compression: Off
    Access Point Name (APN): ctwap
  Profile index: 3
    PDP Type: IPv4
    Header Compression: Off
    Data Compression: Off
    Access Point Name (APN): WONET
Network Information:
  Current Service Status: Emergency
  Current Roaming Status: Roaming
  Current Data Bearer Technology: LTE
  Network Selection Mode: Unknown
Radio Information:
  Technology Preference: LTE only
  Technology Selected: LTE
LTE related info:
  Current RSSI: 99
Modem Security Information:
  SIM Status: Not insert
```

Table 1 Command output

Field	Description
Model	Modem name.
International Mobile Equipment Identity (IMEI)	IMEI serial number of the modem.
Modem Status	Status of the modem: • **Online**—The modem is powered on. • **Offline**—The modem is powered off or in lower power mode. The cellular interface is unavailable.
Profile Information	Profile settings for the 4G modem.
Profile index	Index of the profile for modem.
PDP Type	PDP type, displayed only when Profile 1 is **Active**: • IPv4. • IPv6. • PPP (transparent transmission).
Header Compression	PDP header compression status • On. • Off.

Field	Description
Data Compression	PDP data compression status: • On. • Off.
Current Service Status	Service status of the modem: • **Limited**—The modem is not in the coverage of the selected network. The cellular interface is not available. • **Service available**—The modem is providing services correctly. • **Emergency**—The modem is providing limited services. The cellular interface is not available. • **No service**—The modem cannot provide services. The cellular interface is not available. • **Low power**—The modem is in low power mode. The cellular interface is not available.
Current Roaming Status	Roaming status: • Roaming. • Home.
Current Data Bearer Technology	Current data carrier technology: • CDMA2000 1X. • CDMA2000 HRPD (1xEV-DO). • GSM. • UMTS. • CDMA2000 HRPD (1xEV-DO RevA). • EDGE. • HSDPA and WCDMA. • WCDMA and HSUPA. • HSDPA and HSUPA. • LTE. • CDMA2000 EHRPD. • HSDPA+ and WCDMA. • HSDPA+ and HSUPA. • DC_HSDPA+ and WCDMA. • DC_HSDPA+ and HSUPA. • HSDPA+ and 64QAM. • HSDPA+, 64QAM and HSUPA. • TDSCDMA. • TDSCDMA and HSDPA. • Unknown.
Network Selection Mode	Network selection mode • Manual. • Automatic.
Mobile Country Code (MCC)	The MCC is displayed if the modem has found the network.
Mobile Network Code (MNC)	The MNC is displayed if the modem is successfully registered with a mobile network.
Location Area Code (LAC)	The LAC is displayed if the modem is successfully registered with a mobile network.
Cell ID	The Cell ID is displayed if the modem is successfully registered with a mobile network.

Field	Description
Radio Information	Radio communication information.
Technology Preference	Network connecting preference: • **AUTO**—Connects to a network automatically. • **GSM only**—Connects to a GSM network only. • **GSM precedence**—Connects to a GSM network with preference. • **WCDMA only**—Connects to a WCDMA network only. • **WCDMA precedence**—Connects to a WCDMA network with preference. • **TD-SCDMA only**—Connects to a TD-SCDMA network only. • **TD-SCDMA precedence**—Connects to a TD-SCDMA network with preference. • **EVDO**—Connects to a CDMA-EVDO network only. • **1x RTT**—Connects to a CDMA-1x RTT network only. • **1xRTT/EVDO HYBRID**—Connects to the CDMA-EVDO and CDMA-1x RTT hybrid networks only. • **LTE only**—Connects to an LTE network only.
Technology Selected	Current network: • **GSM**—Has connected to a GSM network. • **WCDMA**—Has connected to a WCDMA network. • **TD-SCDMA**—Has connected to a TD-SCDMA network. • **EVDO**—Has connected to a CDMA-EVDO network. • **1Xrtt**—Has connected to a CDMA-1x RTT network. • **1xRTT/EVDO HYBRID**—Has connected to the CDMA-EVDO and CDMA-1x RTT networks. • **LTE**—Has connected to an LTE network.
LTE related info	Information about the LTE network.
Current RSSI	Current RSSI: • An RSSI value in the range of –110 dBm and –51 dBm. • **Unknown**—No signal. The cellular interface is unavailable.
Current RSRQ	Reference Signal Received Quality.
Current RSRP	Reference Signal Receiving Power.
Current SNR	Signal to noise ratio.
Tx Power	Transmitting power.
Modem Security Information	Information about modem security.
PIN Verification	PIN authentication status: • Disabled. • Enabled. • Unknown.
PIN Status	PIN status: • **Ready**—The SIM card is ready. • **PIN Requirement**—Requires you to execute the **`pin verify`** command to enter the PIN for PIN verification. • **PUK Requirement**—Requires you to execute the **`pin unlock`** command to unlock the SIM or UIM card.
SIM Status	SIM card status: • **OK**—The SIM card is normal. • **Network Reject**—The SIM card is denied access to the network. The

Field	Description
	cellular interface is not available. • **Not Insert**—The SIM card is absent. The cellular interface is not available. • **Not Initialized**—The SIM card status cannot be identified.
ICCID	ID of the SIM card, displayed only when the SIM card status is **OK**.

display controller cellular

Use **display controller cellular** to display information about cellular interfaces.

Syntax

display controller [**cellular** [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

cellular [*interface-number*]: Specifies cellular interfaces or a cellular interface by its number. If you do not specify the **cellular** keyword, this command displays information about all interfaces. If you specify the **cellular** keyword but not the *interface-number* argument, this command displays information about all cellular interfaces.

Usage guidelines

Examples

Display information about Cellular 1/0/6.

```
<Sysname> display controller cellular 1/0/6
Cellular1/0/6
Current state: UP
Description: Cellular1/0/6 Interface
Last clearing of counters: Never
Current system time:2020-04-11 22:31:41 Beijing+08:00:00
Last time when physical state changed to up:2020-04-09 17:16:20 Beijing+08:00:00
Last time when physical state changed to down:2020-04-09 17:16:20 Beijing+08:00:00
Modem status: Present
Capability:
 1 Control channel, 1 ETH channel
Control channel traffic statistics:
 TX: 104366 packets
 RX: 104365 packets
```

Table 2 Command output

Field	Description
Cellular1/0/6 Current state	Status of the interface: • **DOWN(Administratively)**—The interface has been

Field	Description
	administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **UP**—The administrative and physical states of the interface are both up.
Description	Description of the interface.
DM port status	DM status: • Enabled. • Disabled.
Capability: 1 Control channel, 1 PPP channel	Type and number of channels the cellular interface supports: • **1 Control channel**—Supports one control channel. • **1 PPP channel**—Supports one asynchronous serial subchannel. • **1 ETH channel**—Supports one Ethernet subchannel.
Control channel 0 traffic statistics: TX: 0 packets, 0 errors RX: 0 packets, 0 errors	Control channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the control channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the control channel.
PPP channel 0 traffic statistics TX: 0 packets, 0 errors RX: 0 packets, 0 errors	PPP channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the PPP channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the PPP channel.
ETH channel 0 traffic statistics TX: 0 packets, 0 errors RX: 0 packets, 0 errors	Ethernet channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the Ethernet channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the Ethernet channel.

Related commands

reset counters controller cellular

modem reboot

Use **modem reboot** to reboot a 4G modem.

Syntax

modem reboot

Views

Cellular interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command will disconnect the established 3G/4G modem connections. Execute this command with caution.

A 4G modem module can automatically detect running errors and reboot. If the 4G modem fails to reboot by itself, you can use this command to reboot it.

Examples

Manually reboot the 4G modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] modem reboot
```

reset counters controller cellular

Use **reset counters controller cellular** to clear statistics on cellular interfaces.

Syntax

reset counters controller cellular [*interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

cellular [*interface-number*]: Specifies cellular interfaces or a cellular interface by its number. If you do not specify the *interface-number* argument, this command clears statistics on all cellular interfaces. If you specify the *interface-number* argument, this command clears statistics on the specified cellular interface.

Usage guidelines

To collect traffic statistics on an interface during a period of time, first use the **reset counters controller cellular** command to clear the existing statistics on the interface.

Examples

Clear statistics on Cellular 1/0/6.

```
<Sysname> reset counters controller cellular 1/0/6
```

Related commands

display controller cellular

sendat

Use **sendat** to issue a configuration directive to a 4G modem.

Syntax

sendat *at-string*

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

at-string: Specifies a configuration directive string, a string of 1 to 300 characters. This argument can be an AT directive (containing **+++**, **A/**, or be any string beginning with **AT**) or a CNS directive. For more information about AT directives, see the **sendat** command in modem management commands in *Network Connectivity Command Reference*. Table 3 describes the CNS directive samples.

Table 3 CNS directive description

Directive	Description
CNS*n*	Controls the CNS heartbeat debugging switch. • **n = 00000500000000000000**—Enables CNS heartbeat debugging. • **n = 00000800000000000000**—Disables CNS heartbeat debugging.

Usage guidelines

The **sendat** command does not verify the configuration directive. Each time it issues one configuration directive to the 4G modem, lowercase characters are automatically converted to uppercase characters.

One **sendat** command issues one configuration directive. To issue multiple configuration directives to a modem, you must repeat the **sendat** command.

Configuration directives might cause malfunction of a 4G modem. When you issue a configuration directive to the modem, make sure you understand the impact on the 4G modem.

Examples

Issue the **ATD169** directive to the 4G modem to call number 169.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] sendat ATD169
```

Issue the **cns00000500000000000000** directive to the 4G modem to enable CNS heartbeat debugging.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] sendat cns00000500000000000000
```

shutdown

Use **shutdown** to shut down a cellular interface.

Use **undo shutdown** to bring up a cellular interface.

Syntax

shutdown

undo shutdown

Default

The cellular interface is up.

Views

Cellular interface view

Predefined user roles

network-admin

Examples

Shut down Cellular 1/0/6。

```
<Sysname> system-view
[Sysname] interface cellular 1/0/6
[Sysname-Cellular1/0/6] shutdown
```

sim switch-to

Use **sim switch-to** to specify the primary or secondary SIM card.

Syntax

sim switch-to *card-number*

Default

The primary SIM card is used.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

card-number: Specifies a SIM card by its slot number. The value is 0 or 1. 0 represents the primary SIM card. 1 represents the secondary SIM card.

Usage guidelines

CAUTION:

This command might cause traffic interruption. Be aware of the impact of this command before executing it.

On a device that uses dual SIM card, you can execute this command to specify the use of the secondary SIM card when one of the following problems occurs:

- The 4G link signals of the primary SIM card are weak.
- The service provider network that the primary SIM card connects to is unavailable.
- The primary SIM card has failed.

If the issues of the primary SIM card are resolved, you can use this command to specify the use of the primary SIM card.

Examples

Specify the secondary SIM card for the device.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] sim switch-to 1
```

4G modem-specific management commands

apn-profile

Use **apn-profile** to create a 4G modem profile.

Use **undo apn-profile** to remove a 4G modem profile.

Syntax

apn-profile *profile-name*

undo apn-profile *profile-name*

Default

No 4G modem profile exists.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a 4G modem profile name.

Usage guidelines

A 4G modem profile takes effect only after you apply the profile to a 4G interface. To remove a 4G modem profile, you must first remove the association between the profile and the 4G interface.

Examples

Create 4G modem profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
```

bandwidth

Use **bandwidth** to configure the expected bandwidth for an Eth-channel interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Examples

Set the expected bandwidth for Eth-channel 1/0/6:0 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0] bandwidth 1000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Eth-channel interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command before using it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands. Then, use their **undo** forms or follow the command reference to individually restore their default settings. If your restoration attempt fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Eth-channel 1/0/6:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0] default
```

description

Use **description** to configure the description of an Eth-channel interface.

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

Syntax

description *text*

undo description

Default

The description for an Eth-channel interface is in the *interface name* Interface format, for example, Echannel 1/0/6:0 Interface.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

text: Sets an interface description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the description of an interface for easy identification and management purposes.

You can use the **display interface** command to view the description for an interface.

Examples

Configure the description for Eth-channel 1/0/6:0 as **Echannel-interface**.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0] description Echannel-interface
```

display interface eth-channel

Use **display interface eth-channel** to display information about the specified or all Eth-channel interfaces.

Syntax

display interface [**eth-channel** [*channel-id*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

eth-channel [*channel-id*]: Specifies Eth-channel interfaces or an Eth-channel interface by its number. If you do not specify the **eth-channel** keyword, the command displays information about all interfaces. If you specify the **eth-channel** keyword but not the *channel-id* argument, this command displays information about all Eth-channel interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed information about Eth-channel 1/0/6:0.

```
<Sysname> display interface eth-channel 1/0/6:0
Eth-channel1/0/6:0
Current state: DOWN
Line protocol state: DOWN
Description: Eth-channel1/0/6:0 Interface
```

```
Bandwidth: 1000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 00a0-d5ff-ff00
IPv6 packet frame type: Ethernet II, hardware address: 00a0-d5ff-ff00
Output queue - Urgent queuing: Size/Length/Discards 0/1024/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last link flapping: 00:00:00
Input:
  0 packets, 0 bytes
  0 broadcasts, 0 multicasts, 0 unicasts, 0 pauses
  0 errors, 0 runts, 0 giants
  0 CRC, 0 overruns
  0 drops, 0 no buffers
Output:
  0 packets, 0 bytes
  0 broadcasts, 0 multicasts, 0 unicasts, 0 pauses
  0 errors, 0 underruns, 0 collisions
  0 deferred, 0 lost carriers
```

Display brief information about Eth-channel 1/0/6:0.

```
<Sysname> display interface eth-channel 1/0/6:0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Echannel1/0/6:0      UP   UP(s)    192.168.80.239
```

Display information about all Eth-channel interfaces in down state and the causes.

```
<Sysname> display interface eth-channel brief down
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Echannel1/0/6:0      ADM  Administratively
```

Table 4 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of

Field	Description
	null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description for the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum Transmit Unit	MTU of the interface.
Internet protocol processing: disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet Address is 192.168.1.200/24 Primary	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address..
IP Packet Frame Type	IPv4 packet framing format.
Hardware Address	MAC address of the interface.
IPv6 Packet Frame Type	IPv6 packet framing format.
Output queue - Urgent queuing: Size/Length/Discards	Packet statistics for urgent queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.
Output queue - Protocol queuing: Size/Length/Discards	Packet statistics for protocol queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.
Output queue - FIFO queuing: Size/Length/Discards	Packet statistics for FIFO queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **`reset counters interface`** command. If statistics about the interface have never been cleared by using the **`reset counters interface`** command since the device started, this field displays **Never**.
Last 300 seconds input rate	Average input rate during the last 300 seconds: • **bytes/sec**—Average number of received bytes per second. • **bits/sec**—Average number of received bits per second. • **packets/sec**—Average number of received packets per second.
Last 300 seconds output rate	Average output rate over the last 300 seconds: • **bytes/sec**—Average number of sent bytes per second. • **bits/sec**—Average number of sent bits per second. • **packets/sec**—Average number of sent packets per second.

Field	Description
Input: 0 packets, 0 bytes, 0 buffers	Incoming packet statistics: • **0 packets**—Packet number. • **0 bytes**—Packet size in bytes. • **0 buffers**—Number of buffered units.
Output: 0 packets, 0 bytes	Outgoing packet statistics: • **0 packets**—Packet number. • **0 bytes**—Packet size in bytes.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Main IP	Main IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of the interface to be **DOWN**. The value of the field varies by device model. **Administratively** represents that the interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

eth-channel

Use **eth-channel** to channelize a cellular interface into an Eth-channel interface.

Use **undo eth-channel** to remove the Eth-channel interface channelized from a cellular interface.

Syntax

eth-channel *channel-number*

undo eth-channel *channel-number*

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

channel-number: Specifies an Eth-channel interface by its number. The value is 0.

Usage guidelines

This command names the Eth-channel interface channelized from a cellular interface as **eth-channel** *cellular-number*:*channel-number.*

Examples

Channelize Cellular 1/0/6 into an Eth-channel interface.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/6
[Sysname-Cellular1/0/6] eth-channel 0
```

interface eth-channel

Use **interface eth-channel** to enter Eth-channel interface view.

Syntax

interface eth-channel *interface-number*

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies an Eth-channel interface by its number.

Examples

Enter Eth-channel 1/0/6:0 interface view.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0]
```

mtu

Use **mtu** to set the maximum transmission unit (MTU) for an interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of an interface is 1500 bytes.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

size: Sets the MTU in bytes. The value range for the *size* argument is 128 to 2000.

Examples

Set the MTU for Eth-channel 1/0/6:0 to 1430 bytes.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0] mtu 1430
```

reset counters interface

Use **reset counters interface** to clear statistics on the specified or all Eth-channel interfaces.

Syntax

reset counters interface [**eth-channel** [*channel-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

eth-channel [*channel-id*]: Specifies Eth-channel interfaces or an Eth-channel interface by its number. If you do not the **eth-channel** keyword, the command clears statistics on all interfaces. If you specify the **eth-channel** keyword but not the *channel-id* argument, this command clears statistics on all Eth-channel interfaces. If you specify both the **eth-channel** keyword and the *channel-id* argument, this command clears statistics on the specified Eth-channel interface.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific period.

Examples

Clear statistics on Eth-channel 1/0/6:0.

```
<Sysname> reset counters interface eth-channel 1/0/6:0
```

shutdown

Use **shutdown** to shut down an Eth-channel interface.

Use **undo shutdown** to bring up an Eth-channel interface.

Syntax

shutdown

undo shutdown

Default

An Eth-channel interface is up.

Views

Eth-channel interface view

Predefined user roles

network-admin

Examples

Shut down Eth-channel 1/0/6:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/6:0
[Sysname-Eth-channel1/0/6:0] shutdown
```

Contents

ARP commands 1

arp check enable 1
arp check log enable 1
arp max-learning-num 2
arp max-learning-number 4
arp static 6
arp timer aging 7
display arp 8
display arp *ip-address* 11
display arp timer aging 11
reset arp 12

Gratuitous ARP commands 14

arp ip-conflict log prompt 14
arp send-gratuitous-arp 14
gratuitous-arp mac-change retransmit 15
gratuitous-arp-learning enable 16
gratuitous-arp-sending enable 16

Proxy ARP commands 18

display local-proxy-arp 18
display proxy-arp 18
local-proxy-arp enable 19
proxy-arp enable 20

ARP fast-reply commands 21

arp fast-reply enable 21

ARP commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

arp check enable

Use **arp check enable** to enable dynamic ARP entry check.

Use **undo arp check enable** to disable dynamic ARP entry check.

Syntax

arp check enable

undo arp check enable

Default

Dynamic ARP entry check is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Dynamic ARP entry check disables a device from supporting dynamic ARP entries with multicast MAC addresses. The device cannot learn dynamic ARP entries containing multicast MAC addresses. You cannot manually add static ARP entries that contain multicast MAC addresses.

When dynamic ARP entry check is disabled, ARP entries containing multicast MAC addresses are supported. The device can learn dynamic ARP entries containing multicast MAC addresses obtained from the ARP packets sourced from a unicast MAC address. You can also manually add static ARP entries containing multicast MAC addresses.

Examples

Enable dynamic ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp check log enable

Use **arp check log enable** to enable the ARP logging feature.

Use **undo arp check log enable** to disable the ARP logging feature.

Syntax

arp check log enable

undo arp check log enable

Default

ARP logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to log ARP events when ARP cannot resolve IP addresses correctly. The log information helps administrators locate and solve problems. The device can log the following ARP events:

- On a proxy ARP-disabled interface, the target IP address of a received ARP packet is not one of the following IP addresses:
  - The IP address of the receiving interface.
  - The public IP address after NAT.
- The sender IP address of a received ARP reply conflicts with one of the following IP addresses:
  - The IP address of the receiving interface.
  - The public IP address after NAT.

The device sends ARP log messages to the information center. You can use the **info-center source** command to specify the log output rules for the information center. For more information about information center, see *System Management Configuration Guide*.

The device can generate a large number of ARP logs. To conserve system resources, enable ARP logging only when you are auditing or troubleshooting ARP events.

Examples

Enable ARP logging.

```
<Sysname> system-view
[Sysname] arp check log enable
```

arp max-learning-num

Use **arp max-learning-num** to set the dynamic ARP learning limit for an interface.

Use **undo arp max-learning-num** to restore the default.

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

Default

The default for this command is the maximum value of the *max-number* argument.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for an interface.

The following compatibility matrixes show the value ranges for the *max-number* argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	0 to 2048
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2508H-PWR-LTE: 0 to 2048 WX2510H: 0 to 2048 WX2510H-F: 0 to 2048 WX2540H: 0 to 3072 WX2540H-F: 0 to 3072 WX2560H: 0 to 6144
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	0 to 6144
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	WX3010H: 0 to 4096 WX3010H-X-PWR: 0 to 3072 WX3010H-L-PWR: 0 to 4096 WX3024H: 0 to 8192 WX3024H-L-PWR: 0 to 4096 WX3024H-F: 0 to 8192
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: 0 to 8192 WX3510H: 0 to 16384 WX3520H: 0 to 32768 WX3520H-F: 0 to 32768 WX3540H: 0 to 40960
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 0 to 20480 WX5540E: 0 to 61440
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	WX5540H: 0 to 61440 WX5560H: 0 to 81920 WX5580H: 0 to 81920
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	0 to 61440

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	0 to 2048
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	0 to 65536
WX5800H series	WX5860H	EWP-WX5860H-GL	0 to 65536

Usage guidelines

An interface can dynamically learn ARP entries. To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn. When the maximum number is reached, the interface stops learning ARP entries.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

Specify VLAN-interface 40 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10
```

Specify GigabitEthernet 1/0/1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10
```

Specify Layer 2 aggregate interface Bridge-Aggregation 1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10
```

arp max-learning-number

Use **arp max-learning-number** to set the dynamic ARP learning limit for a device.

Use **undo arp max-learning-number** to restore the default.

Syntax

In standalone mode:

arp max-learning-number *max-number*

undo arp max-learning-number

In IRF mode:

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

Default

The default for this command is the maximum value of the *max-number* argument.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for a device.

The following compatibility matrixes show the value ranges for the *max-number* argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	0 to 2048
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2508H-PWR-LTE: 0 to 2048 WX2510H-PWR: 0 to 2048 WX2510H-F-PWR: 0 to 2048 WX2540H: 0 to 3072 WX2540H-F: 0 to 3072 WX2560H: 0 to 6144
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	0 to 6144
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	WX3010H: 0 to 4096 WX3010H-X-PWR: 0 to 3072 WX3010H-L-PWR: 0 to 4096 WX3024H: 0 to 8192 WX3024H-L-PWR: 0 to 4096 WX3024H-F: 0 to 8192
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	WX3508H: 0 to 8192 WX3510H: 0 to 16384 WX3520H: 0 to 32768 WX3520H-F: 0 to 32768 WX3540H: 0 to 40960
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 0 to 20480 WX5540E: 0 to 61440
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	WX5540H: 0 to 61440 WX5560H: 0 to 81920 WX5580H: 0 to 81920
Access controller modules	LSUM1WCME0 EWPXM1WCME0	LSUM1WCME0 EWPXM1WCME0	0 to 61440

Hardware series	Model	Product code	Value range
	LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	0 to 2048
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	0 to 65536
WX5800H series	WX5860H	EWP-WX5860H-GL	0 to 65536

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Usage guidelines

A device can dynamically learn ARP entries. To prevent a device from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the device can learn. When the maximum number is reached, the device stops learning ARP entries.

When the *number* argument is set to 0, the device is disabled from learning dynamic ARP entries.

Examples

Set the ARP learning limit to 64 for slot 1.

```
<Sysname> system-view
[Sysname] arp max-learning-number 64 slot 1
```

arp static

Use **arp static** to configure a static ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

Default

No static ARP entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address for the static ARP entry.

mac-address: Specifies a MAC address for the static ARP entry, in the format of H-H-H.

vlan-id: Specifies the ID of a VLAN to which the static ARP entry belongs. The value range is 1 to 4094.

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

Usage guidelines

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries can be short or long.

A resolved short static ARP entry becomes unresolved upon certain events, for example, when the resolved output interface goes down, or the corresponding VLAN or VLAN interface is deleted.

Long static ARP entries are effective or ineffective. Ineffective long static ARP entries cannot be used for packet forwarding. A long static ARP entry is ineffective when any of the following conditions exists:

- The IP address in the entry conflicts with a local IP address.
- No local interface has an IP address in the same subnet as the IP address in the ARP entry.

If you specify the *vlan-id interface-type interface-number* argument, follow these restrictions and guidelines:

- The interface can be an Ethernet interface or an aggregate interface.
- The VLAN and VLAN interface must already exist. The specified Ethernet interface must belong to the specified VLAN.
- The IP address of the VLAN interface and the IP address specified by the *ip-address* argument must be on the same network.
- If a VLAN or VLAN interface is deleted, a long static ARP entry for the VLAN is deleted and a resolved short static ARP entry for the VLAN becomes unresolved.

Examples

Configure a long static ARP entry that contains IP address 202.38.10.2, MAC address 00e0-fc01-0000, and output interface GigabitEthernet 1/0/1 in VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

Related commands

display arp

reset arp

arp timer aging

Use **arp timer aging** to set the aging timer for dynamic ARP entries.

Use **undo arp timer aging** to restore the default.

Syntax

arp timer aging *aging-time*

undo arp timer aging

Default

The aging timer for dynamic ARP entries is 20 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer in minutes. The value range for this argument is 1 to 1440.

Usage guidelines

Each dynamic ARP entry in the ARP table has a limited lifetime, called an aging timer. The aging timer of a dynamic ARP entry is reset each time the dynamic ARP entry is updated. Dynamic ARP entries that are not updated before their aging timers expire are deleted from the ARP table.

Set the aging timer for dynamic ARP entries as needed. For example, when you configure proxy ARP, set a short aging time so that invalid dynamic ARP entries can be deleted in a timely manner.

Examples

Set the aging timer for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

Related commands

display arp timer aging

display arp

Use **display arp** to display ARP entries.

Syntax

In standalone mode:

display arp [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

In IRF mode:

display arp [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP entries for the master device. (In IRF mode.)

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The VLAN ID is in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays ARP entries for all interfaces.

count: Displays the number of ARP entries.

verbose: Displays detailed information about ARP entries.

Usage guidelines

This command displays information about static and dynamic ARP entries, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display all ARP entries.

```
<Sysname> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
 IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
1.1.1.1         02e0-f102-0023 1             GE1/0/1                 --    S
1.1.1.2         00e0-fc00-0001 12            GE1/0/2                 16    D
1.1.1.3         00e0-fe50-6503 vsi1          Tunnel1                 16    D
```

Display detailed information about all ARP entries.

```
<Sysname> display arp all verbose
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP Address: 1.1.1.1             SVLAN/CVLAN: 1000/1001   Aging: --
MAC Address: 02e0-f102-0023     Type: S                  Nickname: 0x0000
Interface/Link ID: GE1/0/1
VPN Instance: --
VXLAN ID: --
VSI Name: --
VSI Interface: --
MPLS PW ID: --
MPLS peer PE address: --
IP Address: 1.1.1.2             SVLAN/CVLAN: --/--       Aging: --
MAC Address: 0015-e944-adc5     Type: D                  Nickname: 0x0000
Interface/Link ID: GE1/0/2
VPN Instance: --
VXLAN ID: --
VSI Name: --
VSI Interface: --
MPLS PW ID: --
MPLS peer PE address: --
```

Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total number of entries : 3
```

Table 1 Command output

Field	Description
IP Address	IP address in an ARP entry.

Field	Description
MAC Address	MAC address in an ARP entry.
VLAN/VSI name	ID of the VLAN to which the ARP entry belongs. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The output interface of the ARP entry does not belong to the VLAN.
Interface/Link ID	Output interface or link ID in the ARP entry. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry.
Aging	Aging time for an ARP entry in minutes. For a static ARP entry, this field always displays hyphens (**--**). The static ARP entry never ages out unless you delete it manually. For a dynamic ARP entry, this field displays hyphens (**--**) if the aging time is unknown.
Type	ARP entry type: • **D**—Dynamic. • **S**—Static. • **O**—OpenFlow. • **R**—Rule. • **I**—Invalid.
SVLAN/CVLAN	ID of the SVLAN or CVLAN to which the ARP entry belongs. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The output interface of the ARP entry does not belong to a SVLAN or CVLAN.
VPN Instance	This field is not supported in the current software version. Name of VPN instance. If no VPN instance is configured for the ARP entry, this field displays hyphens (**--**).
VXLAN ID	This field is not supported in the current software version. ID of the VXLAN to which the ARP entry belongs. VXLAN ID is also called VNI. If the ARP entry does not belong to any VXLAN, this field displays hyphens (**--**).
VSI Name	This field is not supported in the current software version. Name of the VSI to which the ARP entry belongs. If the ARP entry does not belong to any VSI, this field displays hyphens (**--**).
VSI Interface	This field is not supported in the current software version. Name of the gateway interface of the VSI. If no gateway interface is specified for the VSI, this field displays hyphens (**--**).
MPLS PW ID	This field is not supported in the current software version. ID of the PW to which the ARP entry belongs. This field displays two hyphens (**--**) if the ARP entry does not belong to a PW.
MPLS peer PE address	This field is not supported in the current software version. IP address of the remote PE on the PW. This field displays two hyphens (**--**) if the ARP entry does not belong to a PW.
Nickname	This field is not supported in the current software version. Nickname of the ARP entry. The nickname is a string of four hexadecimal numbers, for example, 0x012a.

Field	Description
Total number of entries	Number of ARP entries.

Related commands

arp static

reset arp

display arp *ip-address*

Use **display arp** *ip-address* to display the ARP entry for an IP address.

Syntax

In standalone mode:

display arp *ip-address* [**verbose**]

In IRF mode:

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device. (In IRF mode.)

verbose: Displays the detailed information about the specified ARP entry.

Usage guidelines

The ARP entry information includes the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display the ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
20.1.1.1        00e0-fc00-0001 --            --                      --    S
```

Related commands

arp static

reset arp

display arp timer aging

Use **display arp timer aging** to display the aging timer of dynamic ARP entries.

Syntax

display arp timer aging

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging timer of dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 20 minute(s)(default)
```

Related commands

arp timer aging

reset arp

Use **reset arp** to clear ARP entries from the ARP table.

Syntax

In standalone mode:

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

In IRF mode:

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears ARP entries for the master device. (In IRF mode.)

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ARP entries for all interfaces.

Examples

Clear all static ARP entries.

```
<Sysname> reset arp static
```

Related commands

arp static

display arp

Gratuitous ARP commands

arp ip-conflict log prompt

Use **arp ip-conflict log prompt** to enable IP conflict notification.

Use **undo arp ip-conflict log prompt** to restore the default.

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

Default

IP conflict notification is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable IP conflict notification on the device.

```
<Sysname> system-view
[Sysname] arp ip-conflict log prompt
```

arp send-gratuitous-arp

Use **arp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets on an interface.

Use **undo arp send-gratuitous-arp** to disable the interface from periodically sending gratuitous ARP packets.

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the sending interval in the range of 200 to 200000 milliseconds. The default value is 2000 milliseconds.

Usage guidelines

This feature takes effect on an interface only when the interface has an IP address and the data link layer state of the interface is up.

This feature can send gratuitous ARP requests only for the sending interface's primary IP address or manually configured secondary IP address. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The sending interval for gratuitous ARP packets might be much longer than the set interval when any of the following conditions exist:

- This feature is enabled on multiple interfaces.
- Each interface is configured with multiple secondary IP addresses.
- A small sending interval is configured in the preceding cases.

Examples

Enable VLAN-interface 2 to send gratuitous ARP packets every 300 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300
```

gratuitous-arp mac-change retransmit

Use **gratuitous-arp mac-change retransmit** to set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

Use **undo gratuitous-arp mac-change retransmit** to restore the default.

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

Default

The device sends a gratuitous packet for its MAC address change once only.

Views

System view

Predefined user roles

network-admin

Parameters

times: Specifies the times of retransmitting a gratuitous packet, in the range of 1 to 10.

interval *seconds*: Specifies the interval for retransmitting a gratuitous packet, in the range of 1 to 10 seconds.

Usage guidelines

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet once only by default. Use this command to configure gratuitous ARP retransmission parameters to ensure that the other devices can receive the packet.

After you execute this command, the device will retransmit a gratuitous ARP packet for its MAC address change at the specified interval for the specified times.

Examples

Set the times to 3 and the interval to 5 for retransmitting a gratuitous ARP packet for the device MAC address change.

```
<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

gratuitous-arp-learning enable

Use **gratuitous-arp-learning enable** to enable learning of gratuitous ARP packets.

Use **undo gratuitous-arp-learning enable** to disable learning of gratuitous ARP packets.

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

Default

Learning of gratuitous ARP packets is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The learning of gratuitous ARP packets feature allows a device to maintain its ARP table by creating or updating ARP entries based on received gratuitous ARP packets.

When this feature is disabled, the device uses received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Examples

Enable learning of gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

gratuitous-arp-sending enable

Use **gratuitous-arp-sending enable** to enable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Use **undo gratuitous-arp-sending enable** to disable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

Default

A device does not send gratuitous ARP packets when it receives ARP requests whose sender IP address is on a different subnet.

Views

System view

Predefined user roles

network-admin

Examples

Disable a device from sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

Proxy ARP commands

display local-proxy-arp

Use **display local-proxy-arp** to display the local proxy ARP status.

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the local proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether local proxy ARP is enabled or disabled.

Examples

Display the local proxy ARP status for VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

Related commands

local-proxy-arp enable

display proxy-arp

Use **display proxy-arp** to display the proxy ARP status.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether proxy ARP is enabled or disabled.

Examples

Display the proxy ARP status on VLAN-interface 2.

```
<Sysname> display proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Proxy ARP status: disabled
```

Related commands

proxy-arp enable

local-proxy-arp enable

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

Default

Local proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ip-range *start-ip-address* **to** *end-ip-address*: Specifies the IP address range for which local proxy ARP is enabled. The start IP address must be lower than or equal to the end IP address.

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable local proxy ARP on VLAN-interface 2.

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

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

Enable local proxy ARP on VLAN-interface 2 for an IP address range.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

Related commands

display local-proxy-arp

proxy-arp enable

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

Syntax

proxy-arp enable

undo proxy-arp enable

Default

Proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Examples

Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

Related commands

display proxy-arp

ARP fast-reply commands

arp fast-reply enable

Use **arp fast-reply enable** to enable ARP fast-reply for a VLAN.

Use **undo arp fast-reply enable** to disable ARP fast-reply for a VLAN.

Syntax

arp fast-reply enable

undo arp fast-reply enable

Default

ARP fast-reply is disabled on a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP fast-reply for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp fast-reply enable
```

Contents

IP addressing commands ····· 1

display ip interface ····· 1
display ip interface brief ····· 3
ip address ····· 4
ip address unnumbered ····· 5

IP addressing commands

display ip interface

Use **display ip interface** to display IP configuration and statistics for Layer 3 interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number. If you do not specify an interface, this command displays IP configuration and statistics for all Layer 3 interfaces.

Usage guidelines

Use the **display ip interface** command to display IP configuration and statistics for the specified Layer 3 interface. The statistics include the following information:

- The number of unicast packets, bytes, and multicast packets the interface has sent and received.
- The number of TTL-invalid packets and ICMP packets the interface has received.

The packet statistics helps you locate a possible attack on the network.

If you specify only the interface type, this command displays IP configuration and statistics for all interfaces of this interface type. If you do not specify any optional parameters, this command displays IP configuration and statistics for all Layer 3 interfaces.

Examples

Display IP configuration and statistics for VLAN-interface 10.

```
<Sysname> display ip interface vlan-interface 10
Vlan-interface10 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
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
```

```
Router advert:                  0
Router solicit:                 0
Time exceed:                    0
IP header bad:                  0
Timestamp request:              0
Timestamp reply:                0
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 1 Command output

Field	Description
current state	Physical link state of the interface: • **Administrative DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol current state	Data link layer state of the interface. • **DOWN**—The data link layer protocol is down. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist.
Internet Address	IP address of an interface followed by: • **Primary**—A primary IP address. • **Sub**—A secondary IP address. • **DHCP-Allocated**—An IP address obtained through DHCP. • **BOOTP-Allocated**—An IP address obtained through BOOTP.
Broadcast address	Broadcast address of the subnet attached to an interface.
The Maximum Transmit Unit	MTU of the interface, in bytes.
input packets, bytes, multicasts output packets, bytes, multicasts	All received and sent packets and bytes, and received and sent multicast packets on an interface (statistics start at the device startup).
TTL invalid packet number	Number of TTL-invalid packets received on the interface (statistics start at the device startup).
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad:	Total number of ICMP packets received on the interface (statistics start at the device startup): • Echo reply packets. • Unreachable packets. • Source quench packets. • Routing redirect packets. • Echo request packets. • Router advertisement packets. • Router solicitation packets. • Time exceeded packets. • IP header bad packets.

Field	Description
Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	• Timestamp request packets. • Timestamp reply packets. • Information request packets. • Information reply packets. • Netmask request packets. • Netmask reply packets. • Unknown type packets.

Related commands

display ip interface brief

ip address

display ip interface brief

Use **display ip interface brief** to display brief IP configuration for Layer 3 interfaces.

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, this command displays brief IP configuration for all Layer 3 interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, this command displays brief IP configuration for all Layer 3 interfaces of the specified type.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays a maximum of 16 characters for each interface description. If the description is longer than 16 characters, the first 14 characters are displayed, followed by an ellipsis (...).

Usage guidelines

Information displayed by the command includes the state of the physical and link layer protocols, IP address, and interface descriptions.

Examples

Display brief IP configuration for VLAN interfaces.

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface                Physical Protocol IP Address      Description
Vlan10                   down     down     6.6.6.1         Link to CoreRo...
Vlan2                    down     down     7.7.7.1         --
<Sysname> display ip interface vlan-interface brief description
```

```
*down: administratively down
(s): spoofing  (l): loopback
Interface                Physical Protocol IP Address      Description
Vlan10                   down     down     6.6.6.1         Link to CoreRouter
Vlan2                    down     down     7.7.7.1         --
```

Table 2 Command output

Field	Description
*down: administratively down	The interface is administratively shut down by using the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Interface name.
Physical	Physical state of the interface: • ***down**—The interface is administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface: • **down**—The protocol state of the interface is down. • **down(l)**—The protocol state of the interface is down (loopback). • **up**—The protocol state of the interface is up. • **up(l)**—The protocol state of the interface is up (loopback). • **up(s)**—The protocol state of the interface is up (spoofing).
IP Address	IP address of the interface. If no IP address is configured, this field displays hyphens (**--**).
Description	Description of the interface. If no description is configured, this field displays hyphens (**--**).

Related commands

display ip interface

ip address

ip address

Use **ip address** to assign an IP address to the interface.

Use **undo ip address** to remove the IP address from the interface.

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]]

Default

No IP address is assigned to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of the interface, in dotted decimal notation.

mask-length: Specifies the subnet mask length in the range of 1 to 31. For a loopback interface, the value range is 1 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

sub: Assigns a secondary IP address to the interface.

Usage guidelines

Use the command to assign a primary or secondary IP address to an interface.

An interface can have only one primary IP address. If you execute this command multiple times to specify different primary IP addresses, the most recent configuration takes effect. If the interface connects to multiple subnets, configure primary and secondary IP addresses on the interface so the subnets can communicate with each other through the interface.

You cannot assign secondary IP addresses to an interface that obtains an IP address through BOOTP, DHCP, or PPP address negotiation.

If you do not specify any parameters, the **undo ip address** command removes all IP addresses from the interface. The **undo ip address** *ip-address* { *mask* | *mask-length* } command removes the primary IP address. The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command removes a secondary IP address.

The primary and secondary IP addresses assigned to the interface can be located on the same network segment. Different interfaces on your device must reside on different network segments.

Examples

Assign VLAN-interface 10 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks both 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub
```

Related commands

display ip interface

display ip interface brief

ip address unnumbered

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use **undo ip address unnumbered** to restore the default.

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	No
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H	Yes

Hardware series	Model	Product code	Command compatibility
	WX1840H	EWP-WX1840H-GL	
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

`interface` *`interface-type interface-number`*: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure VLAN-interface 10 to borrow the IP address of VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address unnumbered interface vlan-interface 100
```

Contents

VLAN commands 1

Basic VLAN commands 1
bandwidth 1
default 1
description 2
display interface vlan-interface 3
display vlan 5
display vlan brief 6
interface vlan-interface 7
mtu 9
name 11
reset counters interface vlan-interface 12
service 12
service standby 13
shutdown 14
vlan 15

Port-based VLAN commands 16
display port 16
port 17
port access vlan 18
port hybrid pvid 18
port hybrid vlan 19
port link-type 20
port trunk permit vlan 21
port trunk pvid 22

VLAN group commands 22
display vlan-group 22
vlan-group 23
vlan-list 24

VLAN commands

Basic VLAN commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bandwidth 10000
```

default

Use **default** to restore the default settings for a VLAN interface.

Syntax

default

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] default
```

description

Use **description** to configure the description of a VLAN or VLAN interface.

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

Syntax

description *text*

undo description

Default

For a VLAN, the description is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

For a VLAN interface, the description is the name of the interface. For example, **Vlan-interface1 Interface**.

Views

VLAN view

VLAN interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

To manage VLANs and VLAN interfaces efficiently, configure descriptions for them based on their functions or connections.

Examples

Configure the description of VLAN 2 as **sales-private**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
```

Configure the description of VLAN-interface 2 as **linktoPC56**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

Related commands

display interface vlan-interface

display vlan

display interface vlan-interface

Use **display interface vlan-interface** to display VLAN interface information.

Syntax

display interface [**vlan-interface** [*interface-number*]] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface number. If you do not specify this option, If you specify the **vlan-interface** keyword without specifying an interface, the command displays information about all VLAN interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

Examples

Display information about VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: Ethernet II, hardware address: 000f-e249-8050
IPv6 packet frame type: Ethernet II, hardware address: 000f-e249-8050
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Vlan2                DOWN DOWN     --
```

Table 1 Command output

Field	Description
Vlan-interface2	VLAN interface name.
Current state	Physical link state of the VLAN interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. The VLAN of this VLAN interface does not contain any physical ports in up state. The ports might not be connected correctly or the links might have failed. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the VLAN interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
Description	Description of the VLAN interface.
Bandwidth	Expected bandwidth of the VLAN interface.
Maximum transmission unit	MTU of the VLAN interface.
Internet protocol processing : Disabled	The VLAN interface is not assigned an IP address and cannot process IP packets.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the VLAN interface.
IPv6 packet frame type	IPv6 packet framing format.
Last clearing of counters	The most recent time that the **reset counters interface vlan-interface** command was executed. This field displays **Never** if you have never executed this command.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rates of input packets and output packets in the last 300 seconds (in Bps, bps, and pps).
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the received packets of the interface and the number of the dropped packets.
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the sent packets of the interface and the number of the dropped packets.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up.

Field	Description
	• **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol state of the interface is up. • **DOWN**—The data link layer protocol state of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag.
Primary IP	Primary IP address of the interface.

Related commands

reset counters interface vlan-interface

display vlan

Use **display vlan** to display VLAN information.

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **static**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a VLAN by its ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs.

dynamic: Specifies dynamic VLANs. If you specify this keyword, the command displays the total number of dynamic VLANs and each dynamic VLAN ID. Dynamic VLANs are assigned by a RADIUS server.

static: Specifies static VLANs. If you specify this keyword, the command displays the total number of static VLANs and each static VLAN ID. Static VLANs are manually created.

Examples

Display information about VLAN 2.

```
<Sysname> display vlan 2
 VLAN ID: 2
```

```
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Display information about VLAN 3.

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN type: static
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:   None
 Untagged ports: None
```

Table 2 Command output

Field	Description
VLAN type	VLAN type, static or dynamic.
Route interface	Whether the VLAN interface is configured for the VLAN. • Not configured. • Configured.
Description	Description of the VLAN.
Name	VLAN name.
IP address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **display interface vlan-interface**. • **display this** (VLAN interface view).
Subnet mask	Subnet mask of the primary IP address. This field is available only when an IP address is configured for the VLAN interface.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

vlan

display vlan brief

Use **display vlan brief** to display brief VLAN information.

Syntax

display vlan brief

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief VLAN information.

```
<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                            Port
1         VLAN 0001                       GE1/0/1  GE1/0/2  GE1/0/3  GE1/0/4
                                          GE1/0/5  GE1/0/6  GE1/0/7  GE1/0/8
                                          GE1/0/9  GE1/0/10
2         VLAN 0002
2         VLAN 0002
3         VLAN 0003
```

Table 3 Command output

Field	Description
Default VLAN ID	System default VLAN ID.
Name	VLAN name.
Port	Ports that allow packets from the VLAN to pass through.

interface vlan-interface

Use **interface vlan-interface** to create a VLAN interface and enter its view, or enter the view of an existing VLAN interface.

Use **undo interface vlan-interface** to delete a VLAN interface.

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

Default

No VLAN interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a VLAN interface number in the range of 1 to 4094.

The following compatibility matrixes show the maximum numbers of VLAN interfaces that can be created:

Hardware series	Models	Product code	Maximum numbers of VLAN interfaces
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	4094
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	• WX2508H-PWR-LTE: 4094 • WX2510H-PWR, WX2510H-F-PWR: 16 • WX2540H, WX2540H-F: 48 • WX2560H: 128
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	128
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	• WX3010H-X-PWR: 48 • WX3010H-L-PWR: 32 • WX3010H, WX3024H-L-PWR: 64 • WX3024H, WX3024H-F: 128
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	• WX3508H, WX3510H: 256 • WX3520H, WX3520H-F: 512 • WX3540H: 1024
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	• WX5510E: 1024 • WX5540E: 4094
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	4094
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	• LSQM1WCMX20, LSUM1WCMX20RT, EWPXM2WCMD0F: 3072 • LSUM1WCME0, EWPXM1WCME0, LSQM1WCMX40, LSUM1WCMX40RT, EWPXM1MAC0F:

Hardware series	Models	Product code	Maximum numbers of VLAN interfaces
			4094

Hardware series	Models	Product code	Maximum numbers of VLAN interfaces
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	• WX1804H-PWR: 4 • WX1810H-PWR: 10 • WX1820H: 16 • WX1840H: 40
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	• WX3820H: 512 • WX3840H: 1024
WX5800H series	WX5860H	EWP-WX5860H-GL	4094

Usage guidelines

Create the VLAN before you create the VLAN interface for a VLAN.

Examples

Create VLAN-interface 2, and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

Related commands

`display interface vlan-interface`

mtu

Use **`mtu`** to set the MTU for a VLAN interface.

Use **`undo mtu`** to restore the default.

Syntax

`mtu` *`size`*

`undo mtu`

Default

The MTU of a VLAN interface is 1500 bytes.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

`size`: Sets the MTU in the range of 46 to 1748 bytes.

The following matrixes show the value ranges for the MTU:

Hardware series	Models	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	46 to 1748
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2508H-PWR-LTE: 46 to 1748 WX2540H: 46 to 1600 WX2510H-PWR: 46 to 1748 WX2510H-F-PWR: 46 to 1748 WX2540H-F: 46 to 1748 WX2560H: 46 to 1748
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	46 to 1748
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	46 to 1748
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	46 to 1748
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	46 to 1748
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	46 to 1748
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	46 to 1748

Hardware series	Models	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	46 to 1748
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	46 to 1748
WX5800H series	WX5860H	EWP-WX5860H-GL	46 to 1748

Usage guidelines

If you configure both the **mtu** and **ip mtu** commands on a VLAN interface, the MTU set by the **ip mtu** command is used for fragmentation. For more information about the **ip mtu** command, see *Network Connectivity Command Reference*.

Examples

Set the MTU to 1492 bytes for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mtu 1492
```

Related commands

display interface vlan-interface

name

Use **name** to assign a name to a VLAN.

Use **undo name** to restore the default.

Syntax

name *text*

undo name

Default

The name of a VLAN is **VLAN** *vlan-id.* The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

Views

VLAN view

Predefined user roles

network-admin

Parameters

text: Specifies a VLAN name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For 802.1X or MAC authentication, you can specify authorization VLANs by their names or IDs. If a large number of VLANs are configured, use VLAN names to identify them.

Examples

Assign the name **test vlan** to VLAN 2.

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

Related commands

display vlan

reset counters interface vlan-interface

Use **reset counters interface vlan-interface** to clear statistics on a VLAN interface.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface by its number. If you do not specify this option, this command clears statistics on all interfaces. If you specify the **vlan-interface** keyword without specifying an interface, this command clears statistics on all VLAN interfaces.

Usage guidelines

Use this command to clear the history statistics before you collect statistics within a time period.

Examples

Clear statistics on VLAN-interface 2.

```
<Sysname> reset counters interface vlan-interface 2
```

Related commands

display interface vlan-interface

service

Use **service** to specify a primary traffic processing slot for a VLAN interface.

Use **undo service** to restore the default.

Syntax

service slot *slot-number*

undo service slot

Default

No primary traffic processing slot is specified for a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

This command is supported only in IRF mode.

Specify a traffic processing slot for a VLAN interface if all traffic on the VLAN interface must be processed on the same slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots for an interface, traffic on that interface is processed as follows:

- The backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.
- When no specified traffic processing slots are available, the traffic is processed on the slot at which it arrives. Then, the processing slot that first becomes available again takes over.

If you do not specify a primary or a backup traffic processing slot for an interface, traffic on that interface is processed on the slot at which the traffic arrives.

Examples

Specify a primary traffic processing slot for VLAN-interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] service slot 2
```

Related commands

service standby

service standby

Use **service standby** to specify a backup traffic processing slot for an interface.

Use **undo service standby** to restore the default.

Syntax

service standby slot *slot-number*

undo service standby slot

Default

No backup traffic processing slot is specified for an interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

This command is supported on IRF-capable centralized devices.

Specify a traffic processing slot for a VLAN interface if all traffic on the VLAN interface must be processed on the same slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots for an interface, traffic on that interface is processed as follows:

- The backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.
- When no specified traffic processing slots are available, the traffic is processed on the slot at which it arrives. Then, the processing slot that first becomes available again takes over.

If you do not specify a primary or a backup traffic processing slot for an interface, traffic on that interface is processed on the slot at which the traffic arrives.

Examples

Specify a primary and a backup traffic processing slot for VLAN-interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] service slot 2
[Sysname-Vlan-interface2] service standby slot 3
```

Related commands

service

shutdown

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

Syntax

shutdown

undo shutdown

Default

A VLAN interface is not manually shut down.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

When a VLAN interface is not manually shut down, the following guidelines apply to the interface state:

- The VLAN interface is down if all ports in the VLAN are down.
- The VLAN interface is up if one or more ports in the VLAN are up.

When you use this command to shut down a VLAN interface, the VLAN interface remains in DOWN (Administratively) state. In this case, the VLAN interface state is not affected by the state of the ports in the VLAN.

Before you configure parameters for a VLAN interface, use this command to shut it down to prevent the configuration from affecting the network. After you complete the VLAN interface configuration, use the **undo shutdown** command to make the settings take effect.

To troubleshoot a failed VLAN interface, you can use the **shutdown** command and then the **undo shutdown** command on the interface to see whether it recovers.

In a VLAN, the state of each Ethernet port is independent of the state of the VLAN interface.

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

Use **vlan** *vlan-id* to create a VLAN and enter its view, or enter the view of an existing VLAN.

Use **vlan** *vlan-id1* **to** *vlan-id2* to create VLANs *vlan-id1* through *vlan-id2*.

Use **vlan all** to create VLANs 1 through 4094.

Use **undo vlan** to delete the specified VLANs.

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Default

VLAN 1 (system default VLAN) exists.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id1: Specifies a VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range. The *vlan-id1* and *vlan-id2* arguments specify VLAN IDs. The value range for each of the two arguments is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Usage guidelines

You cannot create or delete the system default VLAN (VLAN 1).

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Examples

Create VLAN 2 and enter its view.

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

Create VLANs 4 through 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
```

Related commands

display vlan

Port-based VLAN commands

display port

Use **display port** to display information about hybrid or trunk ports.

Syntax

display port { **hybrid** | **trunk** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hybrid: Specifies hybrid ports.

trunk: Specifies trunk ports.

Examples

Display information about hybrid ports.

```
<Sysname> display port hybrid
Interface            PVID  VLAN Passing
GE1/0/2              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 trunk ports.

```
<Sysname> display port trunk
```

```
Interface            PVID  VLAN Passing
GE1/0/2              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 4 Command output

Field	Description
Interface	Interface name.
PVID	Port VLAN ID.
VLAN Passing	Existing VLANs allowed on the port.
Tagged	VLANs from which the port sends packets without removing VLAN tags.
Untagged	VLANs from which the port sends packets after removing VLAN tags.

port

Use **port** to assign the specified access ports to a VLAN.

Use **undo port** to remove the specified access ports from a VLAN.

Syntax

port *interface-list*

undo port *interface-list*

Default

All ports are in VLAN 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 Ethernet interface items. Each item specifies an Ethernet interface or a range of Ethernet interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

This command is applicable only to access ports. This command cannot assign access ports to or remove access ports from VLAN 1.

By default, all ports are access ports. You can manually configure the port link type. For more information, see "port link-type."

Examples

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

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

Related commands

display vlan

port access vlan

Use **port access vlan** to assign an access port to the specified VLAN.

Use **undo port access vlan** to restore the default.

Syntax

port access vlan *vlan-id*

undo port access vlan

Default

All access ports belong to VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

By default, all access ports belong to VLAN 1. Therefore, this command cannot be used to assign access ports to VLAN 1. To move an access port to VLAN 1, execute the **undo port access vlan** command on the access port.

Before assigning an access port to a VLAN, make sure the VLAN has been created.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

port hybrid pvid

Use **port hybrid pvid** to set the PVID of a hybrid port.

Use **undo port hybrid pvid** to set the PVID of a hybrid port to 1.

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

Default

The PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID of a hybrid port. When you delete the PVID of a hybrid port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local hybrid port and its peer.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, set its PVID to VLAN 100, and assign it to VLAN 100 as an untagged member.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Related commands

port hybrid vlan

port link-type

port hybrid vlan

Use **port hybrid vlan** to assign a hybrid port to the specified VLANs.

Use **undo port hybrid vlan** to remove a hybrid port from the specified VLANs.

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

Default

A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. The specified VLANs must already exist on the device.

tagged: Configures the port as a tagged member of the specified VLANs. A tagged member of a VLAN sends packets from the VLAN without removing VLAN tags.

untagged: Configures the port as an untagged member of the specified VLANs. An untagged member of a VLAN sends packets from the VLAN after removing VLAN tags.

Usage guidelines

A hybrid port can allow multiple VLANs. If you execute this command multiple times on a hybrid port, the hybrid port allows all the specified VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100 as a tagged member.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Related commands

port link-type

port link-type

Use **port link-type** to set the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

Default

Each port is an access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

access: Sets the port link type to access.

hybrid: Sets the port link type to hybrid.

trunk: Sets the port link type to trunk.

Usage guidelines

To change the link type of a port from trunk to hybrid or vice versa, first set the link type to access.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

port trunk permit vlan

Use **port trunk permit vlan** to assign a trunk port to the specified VLANs.

Use **undo port trunk permit vlan** to remove a trunk port from the specified VLANs.

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

Default

A trunk port allows packets only from VLAN 1 to pass through.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs. To prevent unauthorized VLAN users from accessing restricted resources through the port, use the **port trunk permit vlan all** command with caution.

Usage guidelines

A trunk port can allow multiple VLANs. If you execute this command multiple times on a trunk port, the trunk port allows all the specified VLANs.

On a trunk port, packets only from the PVID can pass through untagged.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

Related commands

port link-type

port trunk pvid

Use **port trunk pvid** to set the PVID for a trunk port.

Use **undo port trunk pvid** to restore the default.

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

Default

The PVID of a trunk port is VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID for a trunk port. When you delete the PVID of a trunk port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local trunk port and its peer.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a trunk, set its PVID to VLAN 100, and assign it to VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Related commands

port link-type

port trunk permit vlan

VLAN group commands

display vlan-group

Use **display vlan-group** to display VLAN group information.

Syntax

display vlan-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character. If you do not specify this argument, the command displays information about all VLAN groups.

Examples

Display information about VLAN group **test001**.

```
<Sysname> display vlan-group test001
VLAN group: test001
     VLAN list: 2-4 100 200
```

Display information about all VLAN groups.

```
<Sysname> display vlan-group
VLAN group: rnd
     VLAN list: Null
VLAN group: test001
     VLAN list: 2-4 100 200
```

Table 5 Command output

Field	Description
VLAN group	Name of the VLAN group.
VLAN list	VLAN list in the VLAN group.

Related commands

vlan-group

vlan-list

vlan-group

Use **vlan-group** to create a VLAN group and enter its view, or enter the view of an existing VLAN group.

Use **undo vlan-group** to delete a VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character.

Usage guidelines

A VLAN group includes a set of VLANs. You can add multiple VLAN lists to a VLAN group.

On an authentication server, a VLAN group name represents a group of authorization VLANs. When an 802.1X user passes authentication, the authentication server assigns a VLAN group name to the device. The device then uses the received VLAN group name to match the locally configured VLAN group names. If a match is found, the device selects a VLAN from the group and assigns the VLAN to the user.

An AC can allocate the VLANs in a VLAN group to online clients in sequence, so that clients are evenly distributed in VLANs. For more information about this configuration, see WLAN access in *WLAN Configuration Guide*.

Examples

Create a VLAN group named **test001** and enter VLAN group view.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

Related commands

vlan-list

vlan-list

Use **vlan-list** to add VLANs to a VLAN group.

Use **undo vlan-list** to remove VLANs from a VLAN group.

Syntax

vlan-list *vlan-id-list*

undo vlan-list *vlan-id-list*

Default

No VLANs exist in a VLAN group.

Views

VLAN group view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Examples

Add VLAN 2 through VLAN 4, VLAN 100, and VLAN 200 to VLAN group **test001**.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

Related commands

vlan-group

Contents

DHCPv6 commands 1

Common DHCPv6 commands 1
display ipv6 dhcp duid 1
ipv6 dhcp dscp 1
ipv6 dhcp log enable 2
ipv6 dhcp select 2
DHCPv6 server commands 3
address range 3
class pool 4
default pool 5
display ipv6 dhcp option-group 6
display ipv6 dhcp pool 8
display ipv6 dhcp prefix-pool 10
display ipv6 dhcp server 12
display ipv6 dhcp server conflict 13
display ipv6 dhcp server database 13
display ipv6 dhcp server expired 14
display ipv6 dhcp server ip-in-use 15
display ipv6 dhcp server pd-in-use 17
display ipv6 dhcp server statistics 19
dns-server 20
domain-name 21
if-match 22
ipv6 dhcp apply-policy 24
ipv6 dhcp class 24
ipv6 dhcp option-group 25
ipv6 dhcp policy 26
ipv6 dhcp pool 27
ipv6 dhcp prefix-pool 27
ipv6 dhcp server 28
ipv6 dhcp server apply pool 29
ipv6 dhcp server database filename 30
ipv6 dhcp server database update interval 32
ipv6 dhcp server database update now 33
ipv6 dhcp server database update stop 33
ipv6 dhcp server forbidden-address 34
ipv6 dhcp server forbidden-prefix 35
network 36
option 37
option-group 38
prefix-pool 39
reset ipv6 dhcp server conflict 40
reset ipv6 dhcp server expired 40
reset ipv6 dhcp server ip-in-use 41
reset ipv6 dhcp server pd-in-use 42
reset ipv6 dhcp server statistics 42
sip-server 43
static-bind 44
temporary address range 45
DHCPv6 relay agent commands 46
display ipv6 dhcp relay server-address 46
display ipv6 dhcp relay statistics 47
gateway-list 49
ipv6 dhcp relay gateway 49
ipv6 dhcp relay interface-id 50
ipv6 dhcp relay server-address 51
remote-server 52

reset ipv6 dhcp relay statistics ····53
DHCPv6 client commands ····53
display ipv6 dhcp client ····53
display ipv6 dhcp client statistics ····55
ipv6 address dhcp-alloc ····57
ipv6 dhcp client dscp ····57
ipv6 dhcp client duid ····58
ipv6 dhcp client pd ····59
ipv6 dhcp client stateful ····60
ipv6 dhcp client stateless enable ····61
reset ipv6 dhcp client statistics ····61
DHCPv6 snooping commands ····62
display ipv6 dhcp snooping binding ····62
display ipv6 dhcp snooping binding database ····63
display ipv6 dhcp snooping packet statistics ····64
display ipv6 dhcp snooping trust ····64
ipv6 dhcp snooping binding database filename ····65
ipv6 dhcp snooping binding database update interval ····66
ipv6 dhcp snooping binding database update now ····67
ipv6 dhcp snooping binding record ····68
ipv6 dhcp snooping check request-message ····68
ipv6 dhcp snooping deny ····69
ipv6 dhcp snooping enable ····70
ipv6 dhcp snooping log enable ····70
ipv6 dhcp snooping max-learning-num ····71
ipv6 dhcp snooping option interface-id enable ····71
ipv6 dhcp snooping option interface-id string ····72
ipv6 dhcp snooping option remote-id enable ····73
ipv6 dhcp snooping option remote-id string ····73
ipv6 dhcp snooping rate-limit ····74
ipv6 dhcp snooping trust ····75
reset ipv6 dhcp snooping binding ····75
reset ipv6 dhcp snooping packet statistics ····76

DHCPv6 commands

The MSG series, WX2500H-WiNet series, WAC series, WX2500H-LI series, and AC1000 series access controllers do not support parameters or commands that are available only in IRF mode.

Common DHCPv6 commands

display ipv6 dhcp duid

Use **display ipv6 dhcp duid** to display the DUID of the local device.

Syntax

display ipv6 dhcp duid

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

A DHCP unique identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, server, or relay agent). A DHCPv6 device adds its DUID in a sent packet.

This command displays output only after the DHCPv6 process is running on the device.

Examples

Display the DUID of the local device.

```
<Sysname> display ipv6 dhcp duid
The DUID of this device: 0003000100e0fc005552.
```

ipv6 dhcp dscp

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Use **undo ipv6 dhcp dscp** to restore the default.

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

Default

The DSCP value is 56 in DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value for DHCPv6 packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 dhcp log enable

Use **ipv6 dhcp log enable** to enable DHCPv6 server logging.

Use **undo ipv6 dhcp log enable** to disable DHCPv6 server logging.

Syntax

ipv6 dhcp log enable

undo ipv6 dhcp log enable

Default

DHCPv6 server logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCPv6 server to generate DHCPv6 logs and send them to the information center. The log information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *System Management Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address and prefix allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCPv6 server logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp log enable
```

ipv6 dhcp select

Use **ipv6 dhcp select** to enable the DHCPv6 server or DHCPv6 relay agent on an interface.

Use **undo ipv6 dhcp select** to restore the default.

Syntax

ipv6 dhcp select { **relay** | **server** }

undo ipv6 dhcp select

Default

An interface does not work in the DHCPv6 server mode or in the DHCPv6 relay agent mode. It discards DHCPv6 packets from DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCPv6 relay agent on the interface.

server: Enables the DHCPv6 server on the interface.

Usage guidelines

Before changing the DHCPv6 server mode to the DHCPv6 relay agent mode on an interface, use the following commands to remove IPv6 address/prefix bindings:

- **reset ipv6 dhcp server ip-in-use**
- **reset ipv6 dhcp server pd-in-use**

Do not configure the DHCPv6 client on the interface that has been configured as the DHCPv6 relay agent or DHCPv6 server.

Examples

Enable the DHCPv6 server on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp select server
```

Enable the DHCPv6 relay agent on VLAN-interface 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ipv6 dhcp select relay
```

Related commands

display ipv6 dhcp relay server-address

display ipv6 dhcp server

DHCPv6 server commands

address range

Use **address range** to specify a non-temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo address range

Default

No non-temporary IPv6 address range exists.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Specifies the valid lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not specify a non-temporary IPv6 address range, all unicast addresses on the subnet specified by the **network** command in address pool view are assignable. If you specify a non-temporary IPv6 address range, only the IPv6 addresses in the specified IPv6 address range are assignable.

You can specify only one non-temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

The non-temporary IPv6 address range specified by the **address range** command must be on the subnet specified by the **network** command.

Examples

Configure a non-temporary IPv6 address range from 3ffe:501:ffff:100::10 through 3ffe:501:ffff:100::31 in address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] address range 3ffe:501:ffff:100::10 3ffe:501:ffff:100::31
```

Related commands

display ipv6 dhcp pool

network

temporary address range

class pool

Use **class pool** to specify a DHCPv6 address pool for a DHCPv6 user class.

Use **undo class pool** to restore the default.

Syntax

class *class-name* **pool** *pool-name*

undo class *class-name* **pool**

Default

No DHCPv6 address pool is specified for a DHCPv6 user class.

Views

DHCPv6 policy view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCPv6 user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCPv6 address pool for a DHCPv6 user class in a DHCPv6 policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCPv6 address pool **pool1** for DHCPv6 user class **test** in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] class test pool pool1
```

Related commands

default pool

ipv6 dhcp policy

ipv6 dhcp pool

default pool

Use **default pool** to specify the default DHCPv6 address pool.

Use **undo default pool** to restore the default.

Syntax

default pool *pool-name*

undo default pool

Default

No default DHCPv6 address pool is specified.

Views

DHCPv6 policy view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCPv6 policy, the DHCPv6 server uses the default address pool to assign IPv6 address, IPv6 prefix, or other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IPv6 addresses or prefixes, the assignment fails.

You can specify only one default address pool in a DHCPv6 policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the DHCPv6 address pool **pool1** as the default DHCPv6 address pool in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] default pool pool1
```

Related commands

class pool

ipv6 dhcp policy

display ipv6 dhcp option-group

Use **display ipv6 dhcp option-group** to display information about a DHCPv6 option group.

Syntax

display ipv6 dhcp option-group [*option-group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

option-group-number: Specifies a static or dynamic DHCPv6 option group by its ID. The value range for the option group ID is 1 to 100. If you do not specify an option group, this command displays information about all DHCPv6 option groups.

Usage guidelines

A static DHCPv6 option group is created by using the **ipv6 dhcp option-group** command.

A dynamic DHCPv6 option group is created automatically by a DHCPv6 client after it obtains the DHCPv6 configuration parameters. Dynamic option groups cannot be manually modified or deleted.

Examples

Display information about all DHCPv6 option groups.

```
<Sysname> display ipv6 dhcp option-group
DHCPv6 option group: 1
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
```

```
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
      Interface: Vlan-interface10
      Length: 2 bytes
      Hex: ABCD
DHCPv6 option group: 20
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
      Interface: Vlan-interface10
      Length: 2 bytes
      Hex: ABCD
```

Table 1 Command output

Field	Description
DHCPv6 option group	ID of the DHCPv6 option group.
Type	Types of the DHCPv6 option: • **Static**—Parameter in a static DHCPv6 option group. • **Dynamic (DHCPv6 address allocation)**—Parameter in a dynamic DHCPv6 option group created during IPv6 address acquisition. • **Dynamic (DHCPv6 prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 prefix acquisition.

Field	Description
	• **Dynamic (DHCPv6 address and prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 address and prefix acquisition.
Interface	Interface name.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 dhcp option-group

display ipv6 dhcp pool

Use **display ipv6 dhcp pool** to display information about a DHCPv6 address pool.

Syntax

display ipv6 dhcp pool [*pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified DHCPv6 address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays information about all DHCPv6 address pools.

Examples

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 3FFE:501:FFFF:100::/64
    Preferred lifetime 604800, valid lifetime 2592000
  Prefix pool: 1
    Preferred lifetime 24000, valid lifetime 36000
  Addresses:
    Range: from 3FFE:501:FFFF:100::1
           to 3FFE:501:FFFF:100::99
```

```
    Preferred lifetime 70480, valid lifetime 200000
    Total address number: 153
    Available: 153
    In-use: 0
  Temporary addresses:
    Range: from 3FFE:501:FFFF:100::200
           to 3FFE:501:FFFF:100::210
    Preferred lifetime 60480, valid lifetime 259200
    Total address number: 17
    Available: 17
    In-use: 0
  Static bindings:
    DUID: 0003000100e0fc000001
    IAID: 0000003f
    Prefix: 3FFE:501:FFFF:200::/64
      Preferred lifetime 604800, valid lifetime 2592000
    DUID: 0003000100e0fc00cff1
    IAID: 00000001
    Address: 3FFE:501:FFFF:2001::1/64
      Preferred lifetime 604800, valid lifetime 2592000
  DNS server addresses:
    2::2
  Domain name:
    aaa.com
  SIP server addresses:
    5::1
  SIP server domain names:
    bbb.com
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: Not-available
    Preferred lifetime 604800, valid lifetime 2592000
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 1::/64(Zombie)
    Preferred lifetime 604800, valid lifetime 2592000
```

Table 2 Command output

Field	Description
DHCPv6 pool	Name of the DHCPv6 address pool.
Network	IPv6 subnet for dynamic IPv6 address allocation. If the subnet prefix is ineffective, this field displays **Not-available**. If the subnet prefix becomes ineffective after a configuration recovery (for example, a switchover from the backup to the master), the prefix is marked **(Zombie)**.
Prefix pool	Prefix pool referenced by the address pool.

Field	Description
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.
Addresses	Non-temporary IPv6 address range.
Range	IPv6 address range for dynamic allocation.
Total address number	Total number of IPv6 addresses.
Available	Total number of available IPv6 addresses.
In-use	Total number of assigned IPv6 addresses.
Temporary addresses	Temporary IPv6 address range for dynamic allocation.
Static bindings	Static bindings configured in the address pool.
DUID	Client DUID.
IAID	Client IAID. If no IAID is configured, this field displays **Not configured**.
Prefix	IPv6 address prefix.
Address	Static IPv6 address.
DNS server addresses	DNS server address.
Domain name	Domain name.
SIP server addresses	SIP server address.
SIP server domain names	Domain name of the SIP server.

display ipv6 dhcp prefix-pool

Use **display ipv6 dhcp prefix-pool** to display information about a prefix pool.

Syntax

display ipv6 dhcp prefix-pool [*prefix-pool-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-pool-number: Displays detailed information about a prefix pool specified by its number in the range of 1 to 128. If you do not specify a prefix pool, this command displays brief information about all prefix pools.

Examples

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp prefix-pool
Prefix-pool Prefix                                  Available In-use Static
1           5::/64                                  64        0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
```

```
Prefix-pool Prefix                                  Available In-use Static
2           Not-available                           0         0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
Prefix-pool Prefix                                  Available In-use Static
11          21::/112(Zombie)                        0         64     0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64
Assigned length: 70
Total prefix number: 64
Available: 64
In-use: 0
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: Not-available
Assigned length: 70
Total prefix number: 0
Available: 0
In-use: 0
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64(Zombie)
Assigned length: 70
Total prefix number: 10
Available: 0
In-use: 10
Static: 0
```

Table 3 Command output

Field	Description
Prefix-pool	Prefix pool number.
Prefix	Prefix specified in the prefix pool. If the prefix is ineffective, this field displays **Not-available**. If the prefix becomes ineffective after a configuration recovery (for example, a switchover from the backup to the master), the prefix is marked **(Zombie)**.
Available	Number of available prefixes.
In-use	Number of assigned prefixes.
Static	Number of statically bound prefixes.
Assigned length	Length of assigned prefixes.
Total prefix number	Number of prefixes.

display ipv6 dhcp server

Use **display ipv6 dhcp server** to display DHCPv6 server configuration information.

Syntax

display ipv6 dhcp server [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCPv6 server configuration information for the specified interface. If you do not specify an interface, this command displays DHCPv6 server configuration information for all interfaces.

Examples

Display DHCPv6 server configuration information for all interfaces.

```
<Sysname> display ipv6 dhcp server
Interface            Pool
Vlan-interface2      1
Vlan-interface3      global
```

Display DHCPv6 server configuration information for the interface VLAN-interface 2.

```
<Sysname> display ipv6 dhcp server interface vlan-interface 2
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

Table 4 Command output

Field	Description
Interface	Interface enabled with DHCPv6 server.
Pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Using pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Preference value	Server preference in the DHCPv6 Advertise message. The value range is 0 to 255. The bigger the value is, the higher preference the server has.
Allow-hint	Indicates whether desired address/prefix assignment is enabled.
Rapid-commit	Indicates whether rapid address/prefix assignment is enabled.

display ipv6 dhcp server conflict

Use **display ipv6 dhcp server conflict** to display information about IPv6 address conflicts.

Syntax

display ipv6 dhcp server conflict [**address** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays information about all IPv6 address conflicts.

Usage guidelines

The DHCPv6 server creates IP address conflict information in the following conditions:

- The DHCPv6 client sends a DECLINE packet to the DHCPv6 server to inform the server of an IPv6 address conflict.
- The DHCPv6 server discovers that the only assignable address in the address pool is its own IPv6 address.

Examples

Display information about all address conflicts.

```
<Sysname> display ipv6 dhcp server conflict
IPv6 address                                Detect time
2001::1                                     Apr 25 16:57:20 2019
1::1:2                                      Apr 25 17:00:10 2019
```

Table 5 Command output

Field	Description
IPv6 address	Conflicted IPv6 address.
Detect time	Time when the conflict was discovered.

Related commands

reset ipv6 dhcp server conflict

display ipv6 dhcp server database

Use **display ipv6 dhcp server database** to display information about DHCPv6 binding auto backup.

Syntax

display ipv6 dhcp server database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCPv6 binding auto backup.

```
<Sysname> display ipv6 dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
 Latest write time       :   Feb  8 16:02:23 2014
 Status                  :   Last write succeeded.
```

Table 6 Command output

Field	Description
File name	Name of the DHCPv6 binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCPv6 binding change for the DHCPv6 server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display ipv6 dhcp server expired

Use **display ipv6 dhcp server expired** to display lease expiration information.

Syntax

display ipv6 dhcp server expired [**address** *ipv6-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays lease expiration information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays lease expiration information for all IPv6 addresses.

pool *pool-name*: Displays lease expiration information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays lease expiration information for all DHCPv6 address pools.

Usage guidelines

DHCPv6 assigns the expired IPv6 addresses to DHCPv6 clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display ipv6 dhcp server expired
IPv6 address           DUID                            Lease expiration
2001:3eff:fe80:4caa:   3030-3066-2e65-3230-302e-       Apr 25 17:10:47 2019
37ee:7::1              3130-3234-2d45-7468-6572-
                       6e65-7430-2f31
```

Table 7 Command output

Field	Description
IPv6 address	Expired IPv6 address.
DUID	Client DUID bound to the expired IPv6 address.
Lease expiration	Time when the lease expired.

Related commands

reset ipv6 dhcp server expired

display ipv6 dhcp server ip-in-use

Use **display ipv6 dhcp server ip-in-use** to display binding information for assigned IPv6 addresses.

Syntax

display ipv6 dhcp server ip-in-use [**address** *ipv6-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays binding information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays binding information for all IPv6 addresses.

pool *pool-name*: Displays IPv6 address binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 address binding information for all DHCPv6 address pools.

Examples

Display binding information for all assigned IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use
```

```
Pool: 1
 IPv6 address                              Type     Lease expiration
 2:1::1                                    Auto(O)  Jul 10 19:45:01 2019
Pool: 2
 IPv6 address                              Type      Lease expiration
 1:1::2                                    Static(F) Not available
Pool: 3
 IPv6 address                              Type      Lease expiration
 1:2::1F1                                  Static(O) Oct  9 09:23:31 2019
Pool: 4
 IPv6 address                              Type      Lease expiration
 1:2::2                                    Auto(Z)   Oct  11 09:23:31 2019
```

Display binding information for all assigned IPv6 addresses for the specified DHCPv6 address pool.

```
<Sysname> display ipv6 dhcp server ip-in-use pool 1
Pool: 1
 IPv6 address                              Type      Lease expiration
 2:1::1                                    Auto(O)   Jul 10 22:22:22 2019
 3:1::2                                    Static(C) Jan  1 11:11:11 2019
```

Display binding information for the specified IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use address 2:1::3
Pool: 1
Client: FE80::C800:CFF0:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 address: 2:1::3
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2019 (288 seconds left)
```

Table 8 Command output

Field	Description
Pool	DHCPv6 address pool.
IPv6 address	IPv6 address assigned.
Type	IPv6 address binding types: • **Static(F)**—Free static binding whose IPv6 address has not been assigned. • **Static(O)**—Offered static binding whose IPv6 address has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 address has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 address has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the subnet prefix goes invalid for address allocation

Field	Description
	after a configuration recovery, for example, after a switchover from the backup to the master.
Lease-expiration	Time when the lease of the IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID specified, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 address.
valid lifetime	Valid lifetime in seconds of the IPv6 address.
Expires at	Time when the lease of an IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

reset ipv6 dhcp server ip-in-use

display ipv6 dhcp server pd-in-use

Use **display ipv6 dhcp server pd-in-use** to display binding information for the assigned IPv6 prefixes.

Syntax

display ipv6 dhcp server pd-in-use [**pool** *pool-name* | **prefix** *prefix/prefix-len*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays IPv6 prefix binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 prefix binding information for all DHCPv6 address pools.

prefix *prefix/prefix-len*: Displays binding information for the specified IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command displays binding information for all IPv6 prefixes.

Examples

Display all IPv6 prefix binding information.

```
<Sysname> display ipv6 dhcp server pd-in-use
Pool: 1
 IPv6 prefix                              Type      Lease expiration
 2:1::/24                                 Auto(O)   Jul 10 19:45:01 2019
Pool: 2
```

```
 IPv6 prefix                             Type      Lease expiration
 1:1::/64                                Static(F) Not available
Pool: 3
 IPv6 prefix                             Type      Lease expiration
 1:2::/64                                Static(O) Oct  9 09:23:31 2019
Pool: 4
 IPv6 prefix                             Type      Lease expiration
 12::/80                                 Auto(Z)   Oct 17 09:34:59 2019
```

Display IPv6 prefix binding information for DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Pool: 1
 IPv6 prefix                             Type      Lease expiration
 2:1::/24                                Auto(O)   Jul 10 22:22:22 2019
 3:1::/64                                Static(C) Jan  1 11:11:11 2019
```

Display binding information for the IPv6 prefix 2:1::3/24.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Client: FE80::C800:CFF:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 prefix: 2:1::/24
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2019 (288 seconds left)
```

Table 9 Command output

Field	Description
IPv6 prefix	IPv6 prefix assigned.
Type	Prefix binding types: • **Static(F)**—Free static binding whose IPv6 prefix has not been assigned. • **Static(O)**—Offered static binding whose IPv6 prefix has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 prefix has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 prefix has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the prefix in the prefix pool goes invalid after a configuration recovery, for example, after a switchover from the backup to the master.
Pool	Address pool.
Lease-expiration	Time when the lease of the IPv6 prefix will expire. If the lease will expire after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field

Field	Description
	is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 prefix.
valid lifetime	Valid lifetime in seconds of the IPv6 prefix.
Expires at	Time when the lease of the prefix will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

reset ipv6 dhcp server pd-in-use

display ipv6 dhcp server statistics

Use **display ipv6 dhcp server statistics to** display DHCPv6 packet statistics on the DHCPv6 server.

Syntax

display ipv6 dhcp server statistics [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays DHCPv6 packet statistics for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays DHCPv6 packet statistics for all address pools.

Examples

Display all DHCPv6 packet statistics on the DHCPv6 server.

```
<Sysname> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use               :  1
    Pd-in-use               :  0
    Expired                 :  0
Conflict                    :  0
Packets received            :  1
    Solicit                 :  1
    Request                 :  0
    Confirm                 :  0
    Renew                   :  0
    Rebind                  :  0
    Release                 :  0
    Decline                 :  0
```

```
    Information-request       :  0
    Relay-forward             :  0
Packets dropped               :  0
Packets sent                  :  0
    Advertise                 :  0
    Reconfigure               :  0
    Reply                     :  0
    Relay-reply               :  0
```

Table 10 Command output

Field	Description
Bindings	Number of bindings: • **Ip-in-use**—Total number of address bindings. • **Pd-in-use**—Total number of prefix bindings. • **Expired**—Total number of expired address bindings.
Conflict	Total number of conflicted addresses. If statistics about an address pool are displayed, this field is not displayed.
Packets received	Number of messages received by the DHCPv6 server. The message types include: • Solicit. • Request. • Confirm. • Renew. • Rebind. • Release. • Decline. • Information-request. • Relay-forward. If statistics about an address pool are displayed, this field is not displayed.
Packets dropped	Number of packets discarded. If statistics about an address pool are displayed, this field is not displayed.
Packets sent	Number of messages sent by the DHCPv6 server. The message types include: • Advertise. • Reconfigure. • Reply. • Relay-reply. If statistics about an address pool are displayed, this field is not displayed.

Related commands

`reset ipv6 dhcp server statistics`

dns-server

Use **`dns-server`** to specify a DNS server in a DHCPv6 address pool.

Use **`undo dns-server`** to remove the specified DNS server from a DHCPv6 address pool.

Syntax

`dns-server` *`ipv6-address`*

undo dns-server *ipv6-address*

Default

No DNS server address is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

Usage guidelines

You can use the **dns-server** command to specify up to eight DNS servers in an address pool. A DNS server specified earlier has a higher preference.

Examples

Specify the DNS server address 2:2::3 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

Related commands

display ipv6 dhcp pool

domain-name

Use **domain-name** to specify a domain name in a DHCPv6 address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

You can configure only one domain name in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the domain name **aaa.com** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

Related commands

display ipv6 dhcp pool

if-match

Use **if-match** to configure a match rule for a DHCPv6 user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-ipv6-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCPv6 user class.

Views

DHCPv6 user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 128. A smaller ID represents a higher match priority.

option *option-code*: Specifies a DHCPv6 option by its number in the range of 1 to 65535.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 65534. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches the rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies the mask for the match operation. The mask is a hexadecimal number whose length is an even number in the range of 2 to 256 and must be the same as the *hex-string* length. The DHCPv6 server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-ipv6-address*: Specifies a **link-address** field value. The value is an IPv6 address. A packet matches the rule if its **link-address** field value is the same as that in the rule.

Usage guidelines

If a DHCPv6 request sent by a DHCPv6 client matches a rule in a DHCPv6 user class, the DHCPv6 client matches the user class.

You can configure multiple match rules for a DHCPv6 user class. Each match rule is uniquely identified by a rule ID within its type (option or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.
- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.
- Rules of different IDs cannot have the same rule content.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for the DHCPv6 user class **exam** to match DHCPv6 requests that contain Option 16.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 1 option 16
```

Configure match rule **2** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the highest bit of the fourth byte in Option 16 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 2 option 16 hex 00000080 mask 00000080
```

Configure match rule **3** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the first three bytes of Option 16 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 3 option 16 hex 13ae92 offset 0 length 3
```

Configure match rule **4** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the Option 16 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 option 16 hex 13ae partial
```

Configure match rule **5** for the DHCPv6 user class **exam** to match DHCPv6 requests in which the **link-address** field is 2001::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 relay-agent 2001::1
```

Related commands

ipv6 dhcp class

ipv6 dhcp apply-policy

Use **ipv6 dhcp apply-policy** to apply a DHCPv6 policy to an interface.

Use **undo ipv6 dhcp apply-policy** to restore the default.

Syntax

ipv6 dhcp apply-policy *policy-name*

undo ipv6 dhcp apply-policy

Default

No DHCPv6 policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCPv6 policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCPv6 policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply the DHCPv6 policy **test** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp apply-policy test
```

Related commands

ipv6 dhcp class

ipv6 dhcp class

Use **ipv6 dhcp class** to create a DHCPv6 user class and enter its view, or enter the view of an existing DHCPv6 user class.

Use **undo ipv6 dhcp class** to delete the specified DHCPv6 user class.

Syntax

ipv6 dhcp class *class-name*

undo ipv6 dhcp class *class-name*

Default

No DHCPv6 user classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies a name for the DHCPv6 user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCPv6 user class view, you can use the **if-match** command to configure match rules for user classification.

Examples

Create a DHCPv6 user class **test** and enter DHCPv6 user class view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class test
[Sysname-dhcp6-class-test]
```

Related commands

class pool

ipv6 dhcp policy

if-match

ipv6 dhcp option-group

Use **ipv6 dhcp option-group** to create a static DHCPv6 option group and enter its view.

Use **undo ipv6 dhcp option-group** to delete the specified static DHCPv6 option group.

Syntax

ipv6 dhcp option-group *option-group-number*

undo ipv6 dhcp option-group *option-group-number*

Default

No static DHCPv6 option groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

option-group-number: Assigns an ID to the static option group, in the range of 1 to 100.

Usage guidelines

A static DHCPv6 option group can use the same ID as a dynamic DHCPv6 option group. If a static DHCPv6 option group and a dynamic DHCPv6 option group use the same ID, the static one takes precedence over the dynamic one.

Examples

Create static DHCPv6 option group 1 and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp option-group 1
[Sysname-dhcp6-option-group-1]
```

Related commands

display ipv6 dhcp option-group

ipv6 dhcp policy

Use **ipv6 dhcp policy** to create a DHCPv6 policy and enter its view, or enter the view of an existing DHCPv6 policy.

Use **undo ipv6 dhcp policy** to delete a DHCPv6 policy.

Syntax

ipv6 dhcp policy *policy-name*

undo ipv6 dhcp policy *policy-name*

Default

No DHCPv6 policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the DHCPv6 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IPv6 addresses and other parameters from the specified address pool.

For a DHCPv6 policy to take effect, you must apply it to an interface.

Examples

Create DHCPv6 policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy test
[Sysname-dhcp6-policy-test]
```

Related commands

class pool

default pool

ipv6 dhcp apply-policy

ipv6 dhcp class

ipv6 dhcp pool

Use **ipv6 dhcp pool** to create a DHCPv6 address pool and enter its view, or enter the view of an existing DHCPv6 address pool.

Use **undo ipv6 dhcp pool** to delete the specified DHCPv6 address pool.

Syntax

ipv6 dhcp pool *pool-name*

undo ipv6 dhcp pool *pool-name*

Default

No DHCPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a name for the DHCPv6 address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DHCPv6 address pool stores IPv6 address/prefix and other configuration parameters to be assigned to DHCPv6 clients.

When you delete a DHCPv6 address pool, binding information for the assigned IPv6 addresses and prefixes in the address pool is also deleted.

Examples

Create a DHCPv6 address pool named **pool1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool pool1
[Sysname-dhcp6-pool-pool1]
```

Related commands

class pool

display ipv6 dhcp pool

ipv6 dhcp server apply pool

ipv6 dhcp prefix-pool

Use **ipv6 dhcp prefix-pool** to create a prefix pool and specify the prefix and the assigned prefix length for the pool.

Use **undo ipv6 dhcp prefix-pool** to delete the specified prefix pool.

Syntax

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** { *prefix-number* | *prefix/prefix-len* } **assign-len** *assign-len*

undo ipv6 dhcp prefix-pool *prefix-pool-number*

Default

No prefix pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-pool-number: Specifies a prefix pool number in the range of 1 to 128.

prefix { *prefix-number* | *prefix/prefix-len* }: Specifies a prefix by its ID or in the format of *prefix*/*prefix length*. The value range for the *prefix-number* argument is 1 to 1024. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range is 1 to 128, and the value must be greater than or equal to *prefix-len.* The difference between *assign-len* and *prefix-len* must be no more than 16.

Usage guidelines

Different prefix pools cannot overlap.

To modify a prefix pool, execute the **undo ipv6 dhcp prefix-pool** command to delete the prefix pool, and then execute the **ipv6 dhcp prefix-pool** command.

Deleting a prefix pool clears all prefix bindings from the prefix pool.

When you specify a prefix by its ID, follow these restrictions and guidelines:

- This command does not take effect if the prefix does not exist. This command takes effect after the prefix is created.
- If the prefix that the ID represents is changed, the prefix range in the prefix pool accordingly changes.

Examples

Create IPv6 prefix 88:99::/32 with ID 3. Configure prefix pool 2 with IPv6 prefix 3 and an assigned prefix length of 42. Prefix pool 2 contains 1024 prefixes from 88:99::/42 to 88:99:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp prefix-pool 2 prefix 3 assign-len 42
```

Create prefix pool 1, and specify prefix 2001:0410::/32 with an assigned prefix length of 42. Prefix pool 1 contains 1024 prefixes from 2001:0410::/42 to 2001:0410:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

Related commands

display ipv6 dhcp prefix-pool

prefix-pool

ipv6 dhcp server

Use **ipv6 dhcp server** to configure global address assignment on an interface. The server on the interface uses a global address pool to assign configuration information to a client.

Use **undo ipv6 dhcp server** to restore the default.

Syntax

ipv6 dhcp server { **allow-hint** | **preference** *preference-value* | **rapid-commit** } *

undo ipv6 dhcp server

Default

The server does not support desired address/prefix assignment or rapid address/prefix assignment. The server preference is set to 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. The default value is 0. A greater value represents a higher preference.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

The **allow-hint** keyword enables the server to assign the desired address or prefix to the requesting client. If the desired address or prefix is not included in any global address pool, or is already assigned to another client, the server assigns the client a free address or a prefix. If the **allow-hint** keyword is not specified, the server ignores the desired address or prefix, and selects an address or prefix from a global address pool.

If you use the **ipv6 dhcp server** and **ipv6 dhcp server apply pool** commands on the same interface, the **ipv6 dhcp server apply pool** command takes effect.

Examples

Configure global address assignment on the interface VLAN-interface 2. Use the desired address/prefix assignment and rapid address/prefix assignment, and set the server preference to the highest 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp select

ipv6 dhcp server apply pool

Use **ipv6 dhcp server apply pool** to apply a DHCPv6 address pool to an interface.

Use **undo ipv6 dhcp server apply pool** to restore the default.

Syntax

ipv6 dhcp server apply pool *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *

undo ipv6 dhcp server apply pool

Default

No DHCPv6 address pool is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. The default value is 0. A greater value represents a higher preference.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

Upon receiving a DHCPv6 request, the DHCPv6 server selects an IPv6 address or prefix from the address pool applied to the receiving interface. If no address pool is applied, the server selects an IPv6 address or prefix from a global address pool that matches the IPv6 address of the receiving interface or the DHCPv6 relay agent.

The **allow-hint** keyword enables the server to assign the desired address or prefix to the client. If the desired address or prefix does not exist or is already assigned to another client, the server assigns a free address or prefix. If **allow-hint** is not specified, the server ignores the desired address or prefix, and assigns a free address or prefix.

Only one address pool can be applied to an interface. If you execute this command multiple times, the most recent configuration takes effect.

A non-existing address pool can be applied to an interface, but the server cannot assign any prefix, address, or other configuration information from the address pool until the address pool is created.

Examples

Apply address pool 1 to VLAN-interface 2, configure the address pool to support desired address/prefix assignment and address/prefix rapid assignment, and set the preference to 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp pool

ipv6 dhcp select

ipv6 dhcp server database filename

Use **ipv6 dhcp server database filename** to configure the DHCPv6 server to back up the DHCPv6 bindings to a file.

Use **undo ipv6 dhcp server database filename** to restore the default.

Syntax

ipv6 dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp server database filename

Default

The DHCPv6 server does not back up the DHCPv6 bindings.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file. The URL is a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCPv6 server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **ipv6 dhcp server database update interval** command to change the waiting time. If no DHCPv6 binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCPv6 server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the format of ftp:*//server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the format of tftp:*//server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp**

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename database.dhcp
```

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp** in the working directory of the FTP server at 10::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename url ftp://[10::1]/database.dhcp username 1
password simple 1
```

Related commands

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update interval

Use **ipv6 dhcp server database update interval** to set the waiting time for the DHCPv6 server to update the backup file after a DHCPv6 binding change.

Use **undo ipv6 dhcp server database update interval** to restore the default.

Syntax

ipv6 dhcp server database update interval *interval*

undo ipv6 dhcp server database update interval

Default

The DHCPv6 server waits 300 seconds to update the backup file after a DHCPv6 binding change. If no DHCPv6 binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCPv6 binding is created, updated, or removed, the waiting period starts. The DHCPv6 server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCPv6 binding auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCPv6 server to update the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update interval 600
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update now

Use **ipv6 dhcp server database update now** to manually save the DHCPv6 bindings to the backup file.

Syntax

ipv6 dhcp server database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCPv6 bindings are saved to the backup file.

For this command to take effect, you must configure the DHCPv6 auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Manually save the DHCPv6 bindings to the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update now
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update stop

ipv6 dhcp server database update stop

Use **ipv6 dhcp server database update stop** to terminate the download of DHCPv6 bindings from the backup file.

Syntax

ipv6 dhcp server database update stop

Views

System view

Predefined user roles

network-admin

Usage guidelines

The DHCPv6 server does not provide services during the binding download process. If the connection breaks up during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCPv6 server stops waiting and starts providing address allocation services. You can execute this command to terminate the download immediately.

Manual termination allows the DHCPv6 server to provide services without waiting for the connection to be repaired. The IPv6 addresses and prefixes associated with the undownloaded bindings will be assigned to clients and address conflicts might occur.

Examples

Terminate the download of the backup DHCPv6 bindings.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update stop
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server forbidden-address

Use **ipv6 dhcp server forbidden-address** to exclude IPv6 addresses in the DHCPv6 address pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-address** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*]

undo ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*]

Default

Except for the DHCPv6 server address, all IPv6 addresses in a DHCPv6 address pool are assignable.

Views

System view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address, which cannot be lower than *start-ipv6-address*. If you do not specify an end IPv6 address, only the start IPv6 address is excluded from dynamic allocation. If you specify an end IPv6 address, the IP addresses from *start-ipv6-address* through *end-ipv6-address* are all excluded from dynamic allocation.

Usage guidelines

The IPv6 addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IPv6 address is in a static DHCPv6 binding, the address can still be assigned to the client.

The address or address range specified in the **undo** form of the command must be the same as the address or address range specified in the command. To remove an IP address that has been specified as part of an address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IPv6 address ranges from dynamic allocation.

Examples

Exclude IPv6 addresses of 2001:10:110::1 through 2001:10:110::20 from dynamic assignment.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server forbidden-address 2001:10:110::1 2001:10:110::20
```

Related commands

ipv6 dhcp server forbidden-prefix

static-bind

ipv6 dhcp server forbidden-prefix

Use **ipv6 dhcp server forbidden-prefix** to exclude IPv6 prefixes in the DHCPv6 prefix pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-prefix** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*]

undo ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*]

Default

No IPv6 prefixes in the DHCPv6 prefix pool are excluded from dynamic allocation.

Views

System view

Predefined user roles

network-admin

Parameters

start-prefix/prefix-len: Specifies the start IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128.

end-prefix/prefix-len: Specifies the end IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128. The value for *end-prefix* cannot be lower than that for *start-prefix*. If you do not specify this argument, only the *start-prefix/prefix-len* is excluded from dynamic allocation. If you specify this argument, the prefixes from *start-prefix/prefix-len* to *end-prefix/prefix-len* are all excluded.

Usage guidelines

If the excluded IPv6 prefix is in a static binding, the prefix can still be assigned to the client.

The prefix or prefix range specified in the **undo** form of the command must be the same as the prefix or prefix range specified in the command. To remove a prefix that has been specified as part of a prefix range, you must remove the entire prefix range.

You can execute this command multiple times to exclude multiple IPv6 prefix ranges from dynamic allocation.

Examples

Exclude IPv6 prefixes from 2001:3e11::/32 through 2001:3eff::/32 from dynamic allocation.

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

```
[Sysname] ipv6 dhcp server forbidden-prefix 2001:3e11::/32 2001:3eff::/32
```

Related commands

ipv6 dhcp server forbidden-address

static-bind

network

Use **network** to specify an IPv6 subnet for dynamic allocation in a DHCPv6 address pool.

Use **undo network** to restore the default.

Syntax

network { *prefix/prefix-length* | **prefix** *prefix-number* [*sub-prefix/sub-prefix-length*] } [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*] [**export-route**]

undo network

Default

No IPv6 subnet is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

prefix/prefix-length: Specifies the IPv6 subnet for dynamic allocation. The value range for the *prefix-length* argument is 1 to 128.

prefix *prefix-number*: Specifies an IPv6 prefix by its ID in the range of 1 to 1024.

sub-prefix/*sub-prefix-length*: Specifies an IPv6 sub-prefix and its length. The value range for the *sub-prefix-length* argument is 1 to 128. If the IPv6 prefix is longer than the IPv6 sub-prefix or if you do not specify an IPv6 sub-prefix, the IPv6 subnet defined by the IPv6 prefix is used for dynamic allocation.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

export-route: Advertises the subnet assigned to DHCPv6 clients. If you do not specify this keyword, the subnet will not be advertised.

Usage guidelines

You can specify only one subnet for a DHCPv6 address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

Modifying or removing the **network** command configuration removes assigned addresses in the current address pool.

If you execute the **network export-route** command multiple times, the most recent configuration takes effect.

The **network prefix** command does not take effect if the specified IPv6 prefix does not exist. This command takes effect after the IPv6 prefix is created.

The **network** command defines the IPv6 subnet for dynamic allocation through the *prefix/prefix-length* arguments or the *prefix-number* [*sub-prefix*/*sub-prefix-length*] arguments. The IPv6 subnets cannot be the same in different DHCPv6 address pools.

If the prefix that the ID represents is changed, the IPv6 subnet in this command accordingly changes, and the assigned prefix and address bindings are cleared.

Examples

Specify the subnet 3ffe:501:ffff:100::/64 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use the IPv6 subnet defined by the IPv6 prefix for dynamic allocation.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use IPv6 subnet 88:99:ffff:100::/64 defined by IPv6 prefix 3 and IPv6 sub-prefix 3ffe:501:ffff:100::/64 for dynamic allocation. The first 32 bits of the IPv6 subnet are determined by IPv6 prefix 3. The bits 33 to 64 of the IPv6 subnet are determined by the IPv6 sub-prefix and its length. The prefix length of the IPv6 subnet is the IPv6 sub-prefix length.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3 3ffe:501:ffff:100::/64
```

Related commands

address range

display ipv6 dhcp pool

temporary address range

option

Use **option** to configure a self-defined DHCPv6 option in a DHCPv6 address pool.

Use **undo option** to remove a self-defined DHCPv6 option from a DHCPv6 address pool.

Syntax

option *code* **hex** *hex-string*

undo option *code*

Default

No self-defined DHCPv6 option is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

code: Specifies a number for the self-defined option, in the range of 21 to 65535, excluding 25 through 26, 37 through 40, and 43 through 48.

hex *hex-string*: Specifies the content of the option, a hexadecimal number whose length is an even number in the range of 2 to 256.

Usage guidelines

The DHCPv6 server fills the self-defined option with the specified hexadecimal number and sends it in a response to the client.

You can self-define options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command like **dns-server**. For example, you can use the **option 31 hex 020000000000000000000000000000001** command to define the NTP server address 200::1 for DHCP clients.

If a DHCPv6 option is specified by both the dedicated command and the **option** command, the DHCPv6 server preferentially assigns the content specified by the dedicated command. For example, if a DNS server address is specified by the **dns-server** command and the **option 23** command, the server uses the address specified by **dns-server** command.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 23 that specifies a DNS server address 2001:f3e0::1 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option 23 hex 2001f3e000000000000000000000001
```

Related commands

display ipv6 dhcp pool

dns-server

domain-name

sip-server

option-group

Use **option-group** to specify a DHCPv6 option group for a DHCPv6 address pool.

Use **undo option-group** to restore the default.

Syntax

option-group *option-group-number*

undo option-group

Default

No DHCPv6 option group is specified for a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

option-group--number: Specifies a DHCPv6 option group by its number in the range of 1 to 100.

Examples

Specify DHCPv6 option group 1 for DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option-group 1
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp option-group

prefix-pool

Use **prefix-pool** to apply a prefix pool to a DHCPv6 address pool, so the DHCPv6 server can dynamically select a prefix from the prefix pool for a client.

Use **undo prefix-pool** to remove the prefix pool.

Syntax

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo prefix-pool *prefix-pool-number*

Default

No prefix pool is applied to a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

prefix-pool-number: Specifies a prefix pool by its number in the range of 1 to 128.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime in the range of 60 to 4294967295 seconds. The default value is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime in the range of 60 to 4294967295 seconds. The default value is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

Usage guidelines

Only one prefix pool can be applied to an address pool.

You can apply a prefix pool that has not been created to an address pool. The setting takes effect after the prefix pool is created.

To modify the prefix pool in a DHCPv6 address pool, execute the **undo prefix-pool** command to remove the prefix pool, and then execute the **prefix-pool** command.

Examples

Apply prefix pool 1 to address pool 1, and use the default preferred lifetime and valid lifetime.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1
```

Apply prefix pool 2 to address pool 2, and set the preferred lifetime to one day and the valid lifetime to three days.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 2
[Sysname-dhcp6-pool-2] prefix-pool 2 preferred-lifetime 86400 valid-lifetime 259200
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp prefix-pool

reset ipv6 dhcp server conflict

Use **reset ipv6 dhcp server conflict** to clear IPv6 address conflict information.

Syntax

reset ipv6 dhcp server conflict [**address** *ipv6-address*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command clears all IPv6 address conflict information.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After the conflicts are resolved, you can use the **reset ipv6 dhcp server conflict** command to clear conflict information so that the conflicted addresses can be assigned to clients.

Examples

Clear all IPv6 address conflict information.

```
<Sysname> reset ipv6 dhcp server conflict
```

Related commands

display ipv6 dhcp server conflict

reset ipv6 dhcp server expired

Use **reset ipv6 dhcp server expired** to clear binding information for lease-expired IPv6 addresses.

Syntax

reset ipv6 dhcp server expired [**address** *ipv6-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears binding information for the specified lease-expired IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all lease-expired IPv6 address.

pool *pool-name*: Clears binding information for lease-expired IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for lease-expired IPv6 addresses in all address pools.

Examples

Clear binding information for expired IPv6 address 2001:f3e0::1.

```
<Sysname> reset ipv6 dhcp server expired address 2001:f3e0::1
```

Related commands

display ipv6 dhcp server expired

reset ipv6 dhcp server ip-in-use

Use **reset ipv6 dhcp server ip-in-use** to clear binding information for assigned IPv6 addresses.

Syntax

reset ipv6 dhcp server ip-in-use [**address** *ipv6-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears binding information for the specified assigned IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all assigned IPv6 addresses.

pool *pool-name*: Clears binding information for assigned IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 addresses in all address pools.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 addresses.

```
<Sysname> reset ipv6 dhcp server ip-in-use
```

Clears binding information for assigned IPv6 addresses in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server ip-in-use pool 1
```

Clears binding information for the assigned IPv6 address 2001:0:0:1::1.

```
<Sysname> reset ipv6 dhcp server ip-in-use address 2001:0:0:1::1
```

Related commands

display ipv6 dhcp server ip-in-use

reset ipv6 dhcp server pd-in-use

Use **reset ipv6 dhcp server pd-in-use** to clear binding information for assigned IPv6 prefixes.

Syntax

reset ipv6 dhcp server pd-in-use [**pool** *pool-name* | **prefix** *prefix/prefix-len*]

Views

User view

Predefined user roles

network-admin

Parameters

pool *pool-name*: Clears binding information for assigned IPv6 prefixes in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 prefixes in all address pools.

prefix *prefix/prefix-len*: Clears binding information for the specified assigned IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command clears binding information for all assigned IPv6 prefixes.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 prefixes.

```
<Sysname> reset ipv6 dhcp server pd-in-use
```

Clears binding information for assigned IPv6 prefixes in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

Clears binding information for the assigned IPv6 prefix 2001:0:0:1::/64.

```
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

Related commands

display ipv6 dhcp server pd-in-use

reset ipv6 dhcp server statistics

Use **reset ipv6 dhcp server statistics** to clear DHCPv6 server statistics.

Syntax

reset ipv6 dhcp server statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear DHCPv6 server statistics.

```
<Sysname> reset ipv6 dhcp server statistics
```

Related commands

display ipv6 dhcp server statistics

sip-server

Use **sip-server** to specify the IPv6 address or domain name of a SIP server in the DHCPv6 address pool.

Use **undo sip-server** to remove a SIP server.

Syntax

sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

undo sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

Default

No SIP server address or domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Specifies the IPv6 address of a SIP server.

domain-name *domain-name*: Specifies the domain name of a SIP server, a case-insensitive string of 1 to 50 characters.

Usage guidelines

You can specify up to eight SIP server addresses and eight SIP server domain names in an address pool. A SIP server that is specified earlier has a higher preference.

Examples

Specify the SIP server address **2:2::4** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

Specify the SIP server domain name **bbb.com** in DHCPv6 address pool 1.

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

Related commands

display ipv6 dhcp pool

static-bind

Use **static-bind** to statically bind an IPv6 address or prefix to a client in the DHCPv6 address pool.

Use **undo static-bind** to delete a static binding.

Syntax

static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* } **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* }

Default

No static binding is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

address *ipv6-address*/*addr-prefix-length*: Specifies the IPv6 address and prefix length. The value range for the prefix length is 1 to 128.

prefix *prefix*/*prefix-len*: Specifies the prefix and prefix length. The value range for the prefix length is 1 to 128.

duid *duid*: Specifies a client DUID. The value is an even hexadecimal number in the range of 2 to 256.

iaid *iaid*: Specifies a client IAID. The value is a hexadecimal number in the range of 0 to FFFFFFFF. If you do not specify an IAID, the server does not match the client IAID for prefix assignment.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

You can specify multiple static bindings in a DHCPv6 address pool.

An IPv6 address or prefix can be bound to only one DHCPv6 client.

To modify a static binding, execute the **undo static-bind** command to delete the binding, and then execute the **static-bind** command.

Examples

In address pool 1, bind IPv6 address 2001:0410::/35 to the client DUID 0003000100e0fc005552 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind address 2001:0410::/35 duid 0003000100e0fc005552 iaid A1A1A1A1
```

In address pool 1, bind prefix 2001:0410::/35 to the client DUID 00030001CA0006A400 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid A1A1A1A1
```

Related commands

display ipv6 dhcp pool

temporary address range

Use **temporary address range** to configure a temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo temporary address range** to restore the default.

Syntax

temporary address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo temporary address range

Default

No temporary IPv6 address range is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not execute the **temporary address range** command, the DHCPv6 server does not support temporary address assignment.

You can configure only one temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In DHCPv6 address pool 1, configure a temporary IPv6 address range from 3ffe:501:ffff:100::50 to 3ffe:501:ffff:100::60.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
```

```
[Sysname-dhcp6-pool-1] temporary address range 3ffe:501:ffff:100::50
3ffe:501:ffff:100::60
```

Related commands

display ipv6 dhcp pool

address range

network

DHCPv6 relay agent commands

display ipv6 dhcp relay server-address

Use **display ipv6 dhcp relay server-address** to display DHCPv6 server addresses specified on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay server-address
Interface: Vlan-interface2
 Server address                              Outgoing Interface
 2::3
 3::4                                        Vlan-interface4

Interface: Vlan-interface3
 Server address                              Outgoing Interface
 2::3
 3::4                                        Vlan-interface4
```

Display DHCPv6 server addresses on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan-interface2
 Server address                              Outgoing Interface
 2::3
 3::4                                        Vlan-interface4
```

Table 11 Command output

Field	Description
Server address	DHCPv6 server address specified on the DHCP relay agent.
Outgoing Interface	Output interface of DHCPv6 packets. If no output interface is specified, the device searches the routing table for the output interface.

Related commands

ipv6 dhcp relay server-address

ipv6 dhcp select

display ipv6 dhcp relay statistics

Use **display ipv6 dhcp relay statistics** to display DHCPv6 packet statistics on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 packets statistics on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 packet statistics on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped               :  4
Packets received              :  14
    Solicit                   :  0
    Request                   :  0
    Confirm                   :  0
    Renew                     :  0
    Rebind                    :  0
    Release                   :  0
    Decline                   :  0
    Information-request       :  7
    Relay-forward             :  0
    Relay-reply               :  7
Packets sent                  :  14
    Advertise                 :  0
    Reconfigure               :  0
    Reply                     :  7
```

```
    Relay-forward             :  7
    Relay-reply               :  0
```

Display DHCPv6 packet statistics on the DHCPv6 relay agent on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay statistics interface vlan-interface 2
Packets dropped               :  4
Packets received              :  16
    Solicit                   :  0
    Request                   :  0
    Confirm                   :  0
    Renew                     :  0
    Rebind                    :  0
    Release                   :  0
    Decline                   :  0
    Information-request       :  8
    Relay-forward             :  0
    Relay-reply               :  8
Packets sent                  :  16
    Advertise                 :  0
    Reconfigure               :  0
    Reply                     :  8
    Relay-forward             :  8
    Relay-reply               :  0
```

Table 12 Command output

Field	Description
Packets dropped	Number of discarded packets.
Packets received	Number of received packets.
Solicit	Number of received solicit packets.
Request	Number of received request packets.
Confirm	Number of received confirm packets.
Renew	Number of received renew packets.
Rebind	Number of received rebind packets.
Release	Number of received release packets.
Decline	Number of received decline packets.
Information-request	Number of received information request packets.
Relay-forward	Number of received relay-forward packets.
Relay-reply	Number of received relay-reply packets.
Packets sent	Number of sent packets.
Advertise	Number of sent advertise packets.
Reconfigure	Number of sent reconfigure packets.
Reply	Number of sent reply packets.
Relay-forward	Number of sent Relay-forward packets.
Relay-reply	Number of sent Relay-reply packets.

Related commands

reset ipv6 dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCPv6 clients in a DHCPv6 address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCPv6 address pool.

Syntax

gateway-list *ipv6-address*&<1-8>

undo gateway-list [*ipv6-address*&<1-8>]

Default

No gateway address is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

ipv6-address&<1-8>: Specifies a space-separated list of up to eight addresses.

Usage guidelines

DHCPv6 clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IPv6 address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCPv6 address pool.

Upon receiving a DHCPv6 Solicit or Request from a client that matches a DHCPv6 address pool, the relay agent processes the packet as follows:

- Fills the **link-address** field of the packet with a specified gateway address.
- Forwards the packet to all DHCPv6 servers in the matching DHCPv6 address pool.

The DHCPv6 servers select a DHCPv6 address pool according to the gateway address.

Examples

Specify the gateway address 10::1 in the DHCPv6 address pool **p1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool p1
[Sysname-dhcp6-pool-p1] gateway-list 10::1
```

ipv6 dhcp relay gateway

Use **ipv6 dhcp relay gateway** to specify a gateway address for DHCPv6 clients on the DHCPv6 relay interface.

Use **undo ipv6 dhcp relay gateway** to restore the default.

Syntax

ipv6 dhcp relay gateway *ipv6-address*

undo ipv6 dhcp relay gateway

Default

The first IPv6 address of the relay interface is used as the gateway address for DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies a gateway address. The IPv6 address must be an IPv6 address of the relay interface.

Usage guidelines

The DHCPv6 relay agent uses the specified IPv6 address instead of the first IPv6 address of the relay interface as the gateway address for DHCPv6 clients.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10::1 as the gateway address for DHCPv6 clients on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay gateway 10::1
```

Related commands

gateway-list

ipv6 dhcp relay interface-id

Use **ipv6 dhcp relay interface-id** to specify a padding mode for the Interface-ID option.

Use **undo ipv6 dhcp relay interface-id** to restore the default.

Syntax

ipv6 dhcp relay interface-id { **bas** | **interface** }

undo ipv6 dhcp relay interface-id

Default

The DHCPv6 relay agent fills the Interface-ID option with the interface index of the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

bas: Specifies the BAS mode.

interface: Specifies the interface name mode. This mode pads the Interface-ID option in ASCII code with the interface name and VLAN ID of the interface.

Usage guidelines

Enable the DHCPv6 relay agent on the interface before executing this command. Otherwise, the command does not take effect.

Examples

Specify the BAS mode as the padding mode for the Interface-ID option on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id bas
```

Specify the interface name mode as the padding mode for the Interface-ID option on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id interface
```

ipv6 dhcp relay server-address

Use **ipv6 dhcp relay server-address** to specify a DHCPv6 server on the DHCPv6 relay agent.

Use **undo ipv6 dhcp relay server-address** to remove DHCPv6 server addresses.

Syntax

ipv6 dhcp relay server-address *ipv6-address* [**interface** *interface-type interface-number*]

undo ipv6 dhcp relay server-address [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server address is specified on the DHCPv6 relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DHCPv6 server.

interface *interface-type interface-number*: Specifies an output interface through which the relay agent forwards the DHCPv6 requests to the DHCPv6 server. If you do not specify an output interface, the relay agent looks up the routing table for an output interface.

Usage guidelines

Upon receiving a request from a DHCPv6 client, the interface encapsulates the request into a Relay-forward message and forwards the message to the specified DHCPv6 server.

You can specify a maximum of eight DHCPv6 servers on an interface. The DHCPv6 relay agent forwards DHCP requests to all the specified DHCPv6 servers.

If the DHCPv6 server address is a link-local address or multicast address, you must specify an output interface. If you do not specify an output interface, DHCPv6 packets might fail to reach the DHCPv6 server.

If you do not specify an IPv6 address, the **undo ipv6 dhcp relay server-address** command removes all DHCPv6 server addresses specified on the interface.

Do not enable the DHCPv6 client and the DHCPv6 relay agent on the same interface.

Examples

Enable the DHCPv6 relay agent on VLAN-interface 2 and specify the DHCPv6 server address 2001:1::3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp select relay
[Sysname-Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

Related commands

display ipv6 dhcp relay server-address

ipv6 dhcp select

remote-server

Use **remote-server** to specify DHCPv6 servers for a DHCPv6 address pool.

Use **undo remote-server** to remove DHCPv6 servers from a DHCPv6 address pool.

Syntax

remote-server *ipv6-address* [**interface** *interface-type interface-number*]

undo remote-server [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server is specified for the DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies a DHCPv6 server address.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number for the DHCPv6 relay agent to forward packets to the DHCPv6 server. If you do not specify an outgoing interface, the DHCPv6 relay agent performs a routing table lookup.

Usage guidelines

You can specify a maximum of eight DHCPv6 servers in one DHCPv6 address pool.

If you do not specify any parameters, the **undo remote-server** command removes all DHCPv6 servers in the DHCPv6 address pool.

If a DHCPv6 server address is a link-local address, you must specify an outgoing interface by using the **interface** keyword in this command. If you do not specify an outgoing interface, DHCPv6 packets might fail to reach the DHCPv6 server.

Examples

Specify DHCPv6 server 10::1 for DHCPv6 address pool 0.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 0
[Sysname-dhcp6-pool-0] remote-server 10::1
```

reset ipv6 dhcp relay statistics

Use **reset ipv6 dhcp relay statistics** to clear packets statistics on the DHCPv6 relay agent.

Syntax

reset ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all relay agent statistics.

Examples

Clear packet statistics on the DHCPv6 relay agent.

```
<Sysname> reset ipv6 dhcp relay statistics
```

Related commands

display ipv6 dhcp relay statistics

DHCPv6 client commands

display ipv6 dhcp client

Use **display ipv6 dhcp client** to display DHCPv6 client information.

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all DHCPv6 clients.

Examples

Display the DHCPv6 client information on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2:
  Type: Stateful client requesting address and prefix
    State: OPEN
```

```
Client DUID: 0003000100e002000000
Preferred server:
  Reachable via address: FE80::2E0:1FF:FE00:18
  Server DUID: 0003000100e001000000
IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
  Address: 1:1::2/128
    Preferred lifetime 100 sec, valid lifetime 200 sec
    Will expire on Feb 4 2014 at 15:37:20(288 seconds left)
IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
  Prefix: 12:34::/48
    Preferred lifetime 100 sec, valid lifetime 200 sec
    Will expire on Mar 27 2014 at 08:13:24 (199 seconds left)
DNS server addresses:
  2:2::3
Domain name:
  aaa.com
SIP server addresses:
  2:2::4
SIP server domain names:
  bbb.com
Options:
  Code: 88
    Length: 3 bytes
    Hex: AABBCC
```

Table 13 Command output

Field	Description
Type	Types of DHCPv6 client: • **Stateful client requesting address**—A DHCPv6 client that requests an IPv6 address. • **Stateful client requesting prefix**—A DHCPv6 client that requests an IPv6 prefix. • **Stateful client requesting address and prefix**—A DHCPv6 client that requests an IPv6 address and prefix. • **Stateless client**—A DHCPv6 client that requests configuration parameters other than an IPv6 address and prefix through stateless DHCPv6.
State	Current state of the DHCPv6 client: • **IDLE**—The client is in idle state. • **SOLICIT**—The client is locating a DHCPv6 server. • **REQUEST**—The client is requesting an IPv6 address or prefix. • **OPEN**—The client has obtained an IPv6 address or prefix. • **RENEW**—The client is extending the lease (after T1 and before T2). • **REBIND**—The client is extending the lease (after T2 and before the lease expires). • **RELEASE**—The client is releasing an IPv6 address or prefix. • **DECLINE**—The client is declining an IPv6 address or prefix because of an address or prefix conflict. • **INFO-REQUESTING**—The client is requesting configuration parameters through stateless DHCPv6.
Client DUID	DUID of the DHCPv6 client.

Field	Description
Preferred server	Information about the DHCPv6 server selected by the DHCPv6 client.
Reachable via address	Reachable address for the DHCPv6 client. It is the link local address of the DHCPv6 server or DHCPv6 relay agent.
Server DUID	DUID of the DHCPv6 server.
IA_NA	IA_NA information.
IA_PD	IA_PD information.
IAID	IA identifier.
T1	T1 value in seconds.
T2	T2 value in seconds.
Address	IPv6 address obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting address**.
Prefix	IPv6 prefix obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting prefix**.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.
Will expire on Feb 4 2014 at 15:37:20 (288 seconds left)	Time when the lease expires and the remaining time of the lease. If the lease expires after the year 2100, this field displays **Will expire after 2100**.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client duid

ipv6 dhcp client pd

display ipv6 dhcp client statistics

Use **display ipv6 dhcp client statistics** to display DHCPv6 client statistics.

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays statistics for all DHCPv6 clients.

Examples

Display DHCPv6 client statistics on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client statistics interface vlan-interface 2
Interface                    :  Vlan-interface2
Packets received             :  1
         Reply               :  1
         Advertise           :  0
         Reconfigure         :  0
         Invalid             :  0
Packets sent                 :  5
         Solicit             :  0
         Request             :  0
         Renew               :  0
         Rebind              :  0
         Information-request :  5
         Release             :  0
         Decline             :  0
```

Table 14 Command output

Field	Description
Interface	Interface that acts as the DHCPv6 client.
Packets Received	Number of received packets.
Reply	Number of received reply packets.
Advertise	Number of received advertise packets.
Reconfigure	Number of received reconfigure packets.
Invalid	Number of invalid packets.
Packets sent	Number of sent packets.
Solicit	Number of sent solicit packets.
Request	Number of sent request packets.
Renew	Number of sent renew packets.
Rebind	Number of sent rebind packets.
Information-request	Number of sent information request packets.
Release	Number of sent release packets.
Decline	Number of sent decline packets.

Related commands

reset ipv6 dhcp client statistics

ipv6 address dhcp-alloc

Use **ipv6 address dhcp-alloc** to configure an interface to use DHCPv6 for IPv6 address acquisition.

Use **undo ipv6 address dhcp-alloc** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address and other configuration parameters.

Syntax

ipv6 address dhcp-alloc [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 address dhcp-alloc

Default

An interface does not use DHCPv6 for IPv6 address acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

rapid-commit: Supports rapid address or prefix assignment.

Examples

Configure VLAN-interface 10 to use DHCPv6 for IPv6 address acquisition. Configure the DHCPv6 client to support rapid address assignment and create dynamic DHCPv6 option group 1 for the configuration parameters obtained.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 address dhcp-alloc rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client dscp

Use **ipv6 dhcp client dscp** to set the DSCP value for DHCPv6 packets sent by the DHCPv6 client.

Use **undo ipv6 dhcp client dscp** to restore the default.

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

Default

The DSCP value in DHCPv6 packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of a DHCPv6 packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 client.

```
<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30
```

ipv6 dhcp client duid

Use **ipv6 dhcp client duid** to configure the DHCPv6 client DUID for an interface.

Use **undo ipv6 dhcp client duid** to restore the default.

Syntax

ipv6 dhcp client duid { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo ipv6 dhcp client duid

Default

The interface uses the device bridge MAC address to generate its DHCPv6 client DUID.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 130 characters as the DHCPv6 client DUID.

hex *hex-string*: Specifies a hexadecimal number of 2 to 260 characters as the DHCPv6 client DUID.

mac *interface-type interface-number*: Specifies the MAC address of the specified interface as the DHCPv6 client DUID. The *interface-type interface-number* arguments specify an interface by its type and number.

Usage guidelines

A DHCPv6 client pads its DUID into the Option 1 of the DHCPv6 packet that it sends to the DHCPv6 server. The DHCPv6 server can assign specific IPv6 addresses or prefixes to DHCPv6 clients with specific DUIDs.

The DUID of a DHCPv6 client is the globally unique identifier of the client, so make sure the DUID that you configure is unique.

Examples

Specify the hexadecimal number FFFFFFFF as the DHCPv6 client DUID for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client duid hex ffffffff
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client pd

Use **ipv6 dhcp client pd** to configure an interface to use DHCPv6 for IPv6 prefix acquisition.

Use **undo ipv6 dhcp client pd** to cancel an interface from using DHCPv6, and clear the obtained IPv6 prefix and other configuration parameters.

Syntax

ipv6 dhcp client pd *prefix-number* [**option-group** *option-group-number* | **rapid-commit**]*

undo ipv6 dhcp client pd

Default

An interface does not use DHCPv6 for IPv6 prefix acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address or prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Examples

Configure VLAN-interface10 to use DHCPv6 for IPv6 prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid prefix assignment.

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

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 1 rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client stateful

Use **ipv6 dhcp client stateful** to configure an interface to use DHCPv6 for IPv6 address and prefix acquisition.

Use **undo ipv6 dhcp client stateful** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address, prefix, and other configuration parameters.

Syntax

ipv6 dhcp client stateful prefix *prefix-number* [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 dhcp client stateful

Default

An interface does not use DHCPv6 for IPv6 address and prefix acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

prefix *prefix-number*: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address and prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Usage guidelines

The **ipv6 dhcp client stateful** command takes effect if it is configured with the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands on an interface. You must execute the **undo ipv6 dhcp client stateful** command to have the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands take effect.

Examples

Configure VLAN-interface 10 to use DHCPv6 for IPv6 address and prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid address and prefix assignment.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client stateful prefix 1 rapid-commit option-group
1
```

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client pd

ipv6 dhcp client stateless enable

Use **ipv6 dhcp client stateless enable** to enable stateless DHCPv6.

Use **undo ipv6 dhcp client stateless enable** to disable stateless DHCPv6.

Syntax

ipv6 dhcp client stateless enable

undo ipv6 dhcp client stateless enable

Default

Stateless DHCPv6 is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Stateless DHCPv6 enables the interface to send an Information-request message to the multicast address of all DHCPv6 servers and DHCPv6 relay agents for configuration parameters.

Examples

Enable stateless DHCPv6 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp client stateless enable
```

reset ipv6 dhcp client statistics

Use **reset ipv6 dhcp client statistics** to clear DHCPv6 client statistics.

Syntax

reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCPv6 client statistics.

Examples

Clear all DHCPv6 client statistics.

```
<Sysname> reset ipv6 dhcp client statistics
```

Related commands

display ipv6 dhcp client statistics

DHCPv6 snooping commands

DHCPv6 snooping works between the DHCPv6 client and the DHCPv6 server or between the DHCPv6 client and DHCPv6 the relay agent. DHCPv6 snooping does not work between the DHCPv6 server and the DHCPv6 relay agent.

display ipv6 dhcp snooping binding

Use **display ipv6 dhcp snooping binding** to display DHCPv6 snooping entries.

Syntax

display ipv6 dhcp snooping binding [**address** *ipv6-address* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays the DHCPv6 snooping entry for the specified IPv6 address.

vlan *vlan-id*: Specifies the ID of the VLAN where the IPv6 address resides.

Usage guidelines

If you do not specify any parameters, this command displays all DHCPv6 snooping entries.

Examples

Display all DHCPv6 snooping entries.

```
<Sysname> display ipv6 dhcp snooping binding
1 DHCPv6 snooping entries found.
 IPv6 address     MAC address    Lease       VLAN SVLAN Interface
 ================ ============== =========== ==== ===== ======================
 2::1             00e0-fc00-0006 54          2    N/A   GigabitEthernet1/0/1
```

Table 15 Command output

Field	Description
IPv6 Address	IPv6 address assigned to the DHCPv6 client.
MAC Address	MAC address of the DHCPv6 client.
Lease	Remaining lease duration in seconds.
VLAN	When the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides.

Field	Description
SVLAN	When the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connecting to the DHCPv6 client.

Related commands

ipv6 dhcp snooping binding record

reset ipv6 dhcp snooping binding

display ipv6 dhcp snooping binding database

Use **display ipv6 dhcp snooping binding database** to display information about DHCPv6 snooping entry auto backup.

Syntax

display ipv6 dhcp snooping binding database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCPv6 snooping entry auto backup.

```
<Sysname> display ipv6 dhcp snooping binding database
File name              :   database.dhcp
Username               :
Password               :
Update interval        :   600 seconds
Latest write time      :   Feb 27 18:48:04 2012
Status                 :   Last write succeeded.
```

Table 16 Command output

Field	Description
File name	Name of the DHCPv6 snooping entry backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCPv6 snooping entry change for the DHCPv6 snooping device to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display ipv6 dhcp snooping packet statistics

Use **display ipv6 dhcp snooping packet statistics** to display DHCPv6 packet statistics for DHCPv6 snooping.

Syntax

In standalone mode:

display ipv6 dhcp snooping packet statistics

In IRF mode:

display ipv6 dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DHCPv6 packet statistics for the master device. (In IRF mode.)

Examples

Display DHCPv6 packet statistics for DHCPv6 snooping.

```
<Sysname> display ipv6 dhcp snooping packet statistics
 DHCPv6 packets received                 : 100
 DHCPv6 packets sent                     : 200
 Invalid DHCPv6 packets dropped          : 0
```

Related commands

reset ipv6 dhcp snooping packet statistics

display ipv6 dhcp snooping trust

Use **display ipv6 dhcp snooping trust** to display information about trusted ports.

Syntax

display ipv6 dhcp snooping trust

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about trusted ports.

```
<Sysname> display ipv6 dhcp snooping trust
DHCPv6 snooping is enabled.
 Interface                                   Trusted
```

```
========================          ============
GigabitEthernet1/0/1              Trusted
```

Table 17 Command output

Field	Description
Interface	Interface name.
Trusted	DHCP snooping trusted interface. This field displays **Trusted** if the interface is configured as trusted after the DHCPv6 snooping is enabled.

Related commands

ipv6 dhcp snooping trust

ipv6 dhcp snooping binding database filename

Use **ipv6 dhcp snooping binding database filename** to configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to a file.

Use **undo ipv6 dhcp snooping binding database filename** to disable the auto backup and remove the backup file.

Syntax

ipv6 dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp snooping binding database filename

Default

The DHCPv6 snooping device does not back up DHCPv6 snooping entries.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file. The URL is a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL. The supported path format type varies by server.

username *username*: Specifies the username for accessing the URL of the remote backup file. The username is a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

This command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCPv6 snooping device backs up its snooping entries immediately and runs auto backup. The snooping device, by default, waits 300 seconds after a DHCPv6 snooping entry change to update the backup file. You can use the **ipv6 dhcp snooping binding database update interval** command to change the waiting time. If no DHCPv6 snooping entry changes, the backup file is not updated.

As a best practice, back up the DHCPv6 snooping entries to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCPv6 snooping device malfunction.

When the file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the format of ftp:*//server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the format of tftp:*//server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename database.dhcp
```

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp** in the working directory of the FTP server at 1::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename url ftp://[1::1]/database.dhcp
username 1 password simple 1
```

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp** in the working directory of the TFTP server at 2::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename url tftp://[2::1]/database.dhcp
```

Related commands

ipv6 dhcp snooping binding database update interval

ipv6 dhcp snooping binding database update interval

Use **ipv6 dhcp snooping binding database update interval** to set the waiting time for the DHCPv6 snooping device to update the backup file after a DHCPv6 snooping entry change.

Use **undo ipv6 dhcp snooping binding database update interval** to restore the default.

Syntax

ipv6 dhcp snooping binding database update interval *interval*

undo ipv6 dhcp snooping binding database update interval

Default

The DHCPv6 snooping device waits 300 seconds to update the backup file after a DHCPv6 snooping entry change. If no DHCPv6 snooping entry changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the waiting time in seconds, in the range of 60 to 864000.

Usage guidelines

When a DHCPv6 snooping entry is learned, updated, or removed, the waiting period starts. The DHCPv6 snooping device updates the backup file when the waiting period is reached. All snooping entries changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCPv6 snooping entry auto backup by using the **ipv6 dhcp snooping binding database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCPv6 snooping device to update the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update interval 600
```

Related commands

ipv6 dhcp snooping binding database filename

ipv6 dhcp snooping binding database update now

Use **ipv6 dhcp snooping binding database update now** to manually save DHCPv6 snooping entries to the backup file.

Syntax

ipv6 dhcp snooping binding database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCPv6 snooping entries are saved to the backup file.

This command takes effect only after you configure the DHCPv6 snooping entry auto backup by using the **ipv6 dhcp snooping binding database filename** command.

Examples

Manually save DHCPv6 snooping entries to the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update now
```

Related commands

ipv6 dhcp snooping binding database filename

ipv6 dhcp snooping binding record

Use **ipv6 dhcp snooping binding record** to enable recording DHCPv6 snooping entries.

Use **undo ipv6 dhcp snooping binding record** to disable recording DHCPv6 snooping entries.

Syntax

ipv6 dhcp snooping binding record

undo ipv6 dhcp snooping binding record

Default

Recording of DHCPv6 snooping entries is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

You can configure this command on the ports that are directly connected to the DHCPv6 clients.

This command enables DHCPv6 snooping to record IP-to-MAC information of the DHCPv6 clients (called DHCPv6 snooping entries).

Examples

Enable recording DHCPv6 snooping entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
```

ipv6 dhcp snooping check request-message

Use **ipv6 dhcp snooping check request-message** to enable the DHCPv6-REQUEST check feature.

Use **undo ipv6 dhcp snooping check request-message** to disable the DHCPv6-REQUEST check feature.

Syntax

ipv6 dhcp snooping check request-message

undo ipv6 dhcp snooping check request-message

Default

The DHCPv6-REQUEST check feature is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Use the DHCPv6-REQUEST check feature to protect the DHCPv6 server against DHCPv6 client spoofing attacks. The feature enables the DHCPv6 snooping device to check every received DHCPv6-RENEW, DHCPv6-DECLINE, or DHCPv6-RELEASE message against DHCPv6 snooping entries.

- If any criterion in an entry is matched, the device compares the entry with the message information.
  - If they are consistent, the device considers the message valid and forwards it to the DHCPv6 server.
  - If they are different, the device considers the message forged and discards it.
- If no matching entry is found, the device forwards the message to the DHCPv6 server.

Examples

Enable DHCPv6-REQUEST check.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping check request-message
```

ipv6 dhcp snooping deny

Use **ipv6 dhcp snooping deny** to configure a port as DHCPv6 packet blocking port.

Use **undo ipv6 dhcp snooping deny** to restore the default.

Syntax

ipv6 dhcp snooping deny

undo ipv6 dhcp snooping deny

Default

A port does not block DHCPv6 requests.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

To avoid IPv6 address and prefix acquisition failure, configure a port to block DHCPv6 packets only if no DHCPv6 clients are connected to it.

To enable a port on the snooping device to drop all incoming DHCPv6 requests, configure that port as a DHCPv6 packet blocking port.

Examples

Configure GigabitEthernet 1/0/1 as a DHCPv6 packet blocking port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping deny
```

ipv6 dhcp snooping enable

Use **ipv6 dhcp snooping enable** to enable DHCPv6 snooping.

Use **undo ipv6 dhcp snooping enable** to disable DHCPv6 snooping.

Syntax

ipv6 dhcp snooping enable

undo ipv6 dhcp snooping enable

Default

DHCPv6 snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use the DHCPv6 snooping feature together with trusted port configuration. Trusted ports forward responses from DHCPv6 servers and untrusted ports discard responses from DHCPv6 servers. This mechanism ensures that DHCPv6 clients obtain IPv6 addresses or prefixes from authorized DHCPv6 servers.

When DHCPv6 snooping is disabled, all ports on the device forward responses from DHCPv6 servers.

Examples

Enable DHCPv6 snooping.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

ipv6 dhcp snooping log enable

Use **ipv6 dhcp snooping log enable** to enable DHCPv6 snooping logging.

Use **undo ipv6 dhcp snooping log enable** to disable DHCPv6 snooping logging.

Syntax

ipv6 dhcp snooping log enable

undo ipv6 dhcp snooping log enable

Default

DHCPv6 snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCPv6 snooping device to generate DHCPv6 snooping logs and send them to the information center. The log information helps administrators locate and solve problems.

For information about the log destination and output rule configuration in the information center, see *System Management Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Examples

Enable DHCPv6 snooping logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping log enable
```

ipv6 dhcp snooping max-learning-num

Use **ipv6 dhcp snooping max-learning-num** to set the maximum number of DHCPv6 snooping entries for an interface to learn.

Use **undo ipv6 dhcp snooping max-learning-num** to restore the default.

Syntax

ipv6 dhcp snooping max-learning-num *max-number*

undo ipv6 dhcp snooping max-learning-num

Default

The number of DHCPv6 snooping entries for an interface to learn is not limited.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Sets the maximum number of DHCPv6 snooping entries for an interface to learn. The value range for this argument is 1 to 4294967295.

Usage guidelines

When an interface learns the maximum number of DHCPv6 snooping entries, the interface stops learning DHCPv6 snooping entries. This does not affect the operation of the DHCPv6 snooping feature.

Examples

Configure the Layer 2 Ethernet interface GigabitEthernet 1/0/1 to learn a maximum of 10 DHCPv6 snooping entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping max-learning-num 10
```

ipv6 dhcp snooping option interface-id enable

Use **ipv6 dhcp snooping option interface-id enable** to enable support for the interface-ID option (also called Option 18).

Use **undo ipv6 dhcp snooping option interface-id enable** to disable support for the interface-ID option.

Syntax

ipv6 dhcp snooping option interface-id enable

undo ipv6 dhcp snooping option interface-id enable

Default

Option 18 is not supported.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when DHCPv6 snooping is globally enabled.

Examples

Enable support for Option 18.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option interface-id string

ipv6 dhcp snooping option interface-id string

Use **ipv6 dhcp snooping option interface-id string** to specify the content as the interface ID for Option 18.

Use **undo ipv6 dhcp snooping option interface-id string** to restore the default.

Syntax

ipv6 dhcp snooping option interface-id [**vlan** *vlan-id*] **string** *interface-id*

undo ipv6 dhcp snooping option interface-id [**vlan** *vlan-id*] **string**

Default

The DHCPv6 snooping device uses its DUID as the content for Option 18.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the interface ID for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the interface ID for packets received from the default VLAN.

interface-id: Specifies a string of 1 to 128 characters as the interface ID.

Examples

Specify **company001** as the interface ID.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id string company001
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option interface-id enable

ipv6 dhcp snooping option remote-id enable

Use **ipv6 dhcp snooping option remote-id enable** to enable support for the remote-ID option (also called Option 37).

Use **undo ipv6 dhcp snooping option remote-id enable** to disable support for the remote-ID option.

Syntax

ipv6 dhcp snooping option remote-id enable

undo ipv6 dhcp snooping option remote-id enable

Default

Option 37 is not supported.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when DHCPv6 snooping is globally enabled.

Examples

Enable support for Option 37.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option remote-id string

ipv6 dhcp snooping option remote-id string

Use **ipv6 dhcp snooping option remote-id string** to specify the content as the remote ID for Option 37.

Use **undo ipv6 dhcp snooping option remote-id string** to restore the default.

Syntax

ipv6 dhcp snooping option remote-id [**vlan** *vlan-id*] **string** *remote-id*

undo ipv6 dhcp snooping option remote-id [**vlan** *vlan-id*] **string**

Default

The DHCPv6 snooping device uses its DUID as the content for Option 37.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the remote ID for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the remote ID for packets received from the default VLAN.

remote-id: Specifies a string of 1 to 128 characters as the remote ID.

Examples

Specify **device001** as the remote ID.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id string device001
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option remote-id enable

ipv6 dhcp snooping rate-limit

Use **ipv6 dhcp snooping rate-limit** to enable DHCPv6 snooping packet rate limit on an interface and set the limit value.

Use **undo ipv6 dhcp snooping rate-limit** to disable DHCPv6 snooping packet rate limit.

Syntax

ipv6 dhcp snooping rate-limit *rate*

undo ipv6 dhcp snooping rate-limit

Default

The DHCPv6 snooping packet rate limit is disabled on an interface.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the maximum rate in Kbps.The value range for this argument is 64 to 512.

Usage guidelines

This command takes effect only when DHCPv6 snooping is enabled.

The DHCPv6 packet rate limit feature enables the interface to discard DHCPv6 packets that exceed the maximum rate.

The rate configured on a Layer 2 aggregate interface applies to all members of the aggregate interface. If a member interface leaves the aggregation group, it uses the rate configured in its Ethernet interface view.

Examples

Configure GigabitEthernet 1/0/1 to receive DHCPv6 packets at a maximum rate of 64 Kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping rate-limit 64
```

ipv6 dhcp snooping trust

Use **ipv6 dhcp snooping trust** to configure a port as a trusted port.

Use **undo ipv6 dhcp snooping trust** to restore the default state of a port.

Syntax

ipv6 dhcp snooping trust

undo ipv6 dhcp snooping trust

Default

After you enable DHCPv6 snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Specify the port facing the DHCP server as trusted and specify the other ports as untrusted so DHCP clients can obtain valid IP addresses.

Examples

Specify GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

Related commands

display ipv6 dhcp snooping trust

reset ipv6 dhcp snooping binding

Use **reset ipv6 dhcp snooping binding** to clear DHCPv6 snooping entries.

Syntax

reset ipv6 dhcp snooping binding { **all** | **address** *ipv6-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears the DHCPv6 snooping entry for the specified IPv6 address.

vlan *vlan-id*: Clears DHCPv6 snooping entries for the specified VLAN. If you do not specify a VLAN, this command clears DHCPv6 snooping entries for the default VLAN.

all: Clears all DHCPv6 snooping entries.

Examples

Clear all DHCPv6 snooping entries.

```
<Sysname> reset ipv6 dhcp snooping binding all
```

Related commands

display ipv6 dhcp snooping binding

reset ipv6 dhcp snooping packet statistics

Use **reset ipv6 dhcp snooping packet statistics** to clear DHCPv6 packet statistics for DHCPv6 snooping.

Syntax

In standalone mode:

reset ipv6 dhcp snooping packet statistics

In IRF mode:

reset ipv6 dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears DHCPv6 packet statistics for the master device. (In IRF mode.)

Examples

Clear DHCPv6 packet statistics for DHCPv6 snooping.

```
<Sysname> reset ipv6 dhcp snooping packet statistics
```

Related commands

display ipv6 dhcp snooping packet statistics

Contents

DNS commands 1

display dns domain 1
display dns host 1
display dns server 3
display ipv6 dns server 3
dns domain 4
dns dscp 5
dns proxy enable 6
dns server 6
dns snooping enable 7
dns source-interface 8
dns spoofing 8
dns trust-interface 9
ip host 10
ipv6 dns dscp 11
ipv6 dns server 11
ipv6 dns spoofing 12
ipv6 host 13
reset dns host 13

DDNS commands 15

ddns apply policy 16
ddns dscp 17
ddns policy 17
display ddns policy 18
interval 19
method 20
password 21
ssl-client-policy 22
url 23
username 25

DNS commands

display dns domain

Use **display dns domain** to display the domain name suffixes.

Syntax

display dns domain [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained domain name suffixes.

Examples

Display the statically configured and dynamically obtained domain name suffixes for the public network.

```
<Sysname> display dns domain
Type:
  D: Dynamic    S: Static

No.     Type    Domain suffix
1       S       com
2       D       net
```

Table 1 Command output

Field	Description
No.	Sequence number.
Type	Domain name suffix type: • **S**—A statically configured domain name suffix. • **D**—A domain name suffix dynamically obtained through DHCP or other protocols.
Domain suffix	Domain name suffixes.

Related commands

dns domain

display dns host

Use **display dns host** to display information about domain name-to-IP address mappings.

Syntax

display dns host [**ip** | **ipv6**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, this command displays domain name-to-IP address mappings of all query types.

Examples

Display domain name-to-IP address mappings of all query types.

```
<Sysname> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name         Type  TTL        Query type   IP addresses
1    sample.com        D     3132       A            192.168.10.1
                                                     192.168.10.2
                                                     192.168.10.3
2    zig.sample.com    S     -          A            192.168.1.1
3    sample.net        S     -          AAAA         FE80::4904:4448
```

Table 2 Command output

Field	Description
No.	Sequence number.
Host name	Domain name.
Type	Domain name-to-IP address mapping type: • **S**—A static mapping configured by the **ip host** or **ipv6 host** command. • **D**—A mapping dynamically obtained through dynamic domain name resolution.
TTL	Time in seconds that a mapping can be stored in the cache. For a static mapping, a hyphen (-) is displayed.
Query type	Query type: A and AAAA.
IP addresses	Replied IP address: • For a type A query, the replied IP address is an IPv4 address. • For a type AAAA query, the replied IP address is an IPv6 address.

Related commands

ip host

ipv6 host

reset dns host

display dns server

Use **display dns server** to display IPv4 DNS server information.

Syntax

display dns server [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv4 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays statically configured and dynamically obtained IPv4 DNS server information.

Examples

Display IPv4 DNS server information for the public network.

```
<Sysname> display dns server
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

Table 3 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IP address	IPv4 address of the DNS server.

Related commands

dns server

display ipv6 dns server

Use **display ipv6 dns server** to display IPv6 DNS server information.

Syntax

display ipv6 dns server [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv6 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained IPv6 DNS server information.

Examples

Display IPv6 DNS server information for the public network.

```
<Sysname> display ipv6 dns server
Type:
  D: Dynamic    S: Static

No. Type  IPv6 address                              Outgoing Interface
1   S     2::2
```

Table 4 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IPv6 address	IPv6 address of the DNS server.
Outgoing Interface	Output interface.

Related commands

ipv6 dns server

dns domain

Use **dns domain** to configure a domain name suffix.

Use **undo dns domain** to delete the specified domain name suffix.

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

Default

No domain name suffix is configured. Only the provided domain name is resolved.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The domain name suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

Usage guidelines

For domain name resolution, the resolver automatically uses the suffix list to supply the missing part of an incomplete name entered by a user.

A domain name suffix applies to both IPv4 DNS and IPv6 DNS.

The system allows a maximum of 16 domain name suffixes for the public network.

Examples

Configure domain name suffix **com** for the public network.

```
<Sysname> system-view
[Sysname] dns domain com
```

Related commands

display dns domain

dns dscp

Use **dns dscp** to set the DSCP value for DNS packets sent by a DNS client or DNS proxy.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value is 0 in DNS packets sent by a DNS client or DNS proxy.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DNS packets.

```
<Sysname> system-view
[Sysname] dns dscp 30
```

dns proxy enable

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to disable DNS proxy.

Syntax

dns proxy enable

undo dns proxy enable

Default

DNS proxy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This configuration applies to both IPv4 DNS and IPv6 DNS.

Examples

Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns server

Use **dns server** to specify the IPv4 address of a DNS server.

Use **undo dns server** to remove the IPv4 address of a DNS server.

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

Default

No DNS server IPv4 address is specified.

Views

System view

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of a DNS server. When you execute the **undo** form of the command in interface view, you must specify this argument.

Usage guidelines

The device sends a DNS query request to the DNS servers in the order their IPv4 addresses are specified.

The system allows a maximum of six DNS server IPv4 addresses for the public network.

If you do not specify an IPv4 address, the **undo dns server** command removes all DNS server IPv4 addresses for the public network.

Examples

Specify DNS server IPv4 address 172.16.1.1.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

Specify DNS server IPv4 address 172.16.1.1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dns server 172.16.1.1
```

Related commands

display dns server

dns snooping enable

Use **dns snooping enable** to enable DNS snooping.

Use **undo dns snooping enable** to disable DNS snooping.

Syntax

dns snooping enable

undo dns snooping enable

Default

DNS snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DNS snooping is applicable to scenarios that use domain name-based policies (such as security policies and bandwidth policies). In such a scenario, the device requires the resolved IP addresses for traffic filtering. Enabled with DNS snooping, the device monitors received DNS requests and replies, and works as follows:

- If the domain name in a DNS request matches a policy, the device records the DNS mapping after receiving the DNS reply, and reports the mapping to the policy for traffic filtering.
- If the domain name does not match a policy, the device does not record the DNS mapping.

DNS snooping works only between the DNS client and DNS server, or the DNS client and DNS proxy.

The DNS snooping and DNS transparent proxy features cannot be both configured.

Examples

Enable DNS snooping.

```
<Sysname> system-view
[Sysname] dns snooping enable
```

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface *interface-type interface-number*

Default

No source interface is specified for DNS packets. The device uses the primary IP address of the output interface of the matching route as the source IP address for a DNS request.

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

This configuration applies to both IPv4 and IPv6.

In IPv4 DNS, the device uses the primary IPv4 address of the specified source interface as the source IP address of a DNS query. In IPv6 DNS, the device selects an IPv6 address of the specified source interface as the source IP address of a DNS query. The method of selecting the IPv6 address is defined in RFC 3484.

The system allows only one source interface for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify VLAN-interface 2 as the source interface for DNS packets on the public network.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface 2
```

dns spoofing

Use **dns spoofing** to enable DNS spoofing and specify the IPv4 address for spoofing DNS requests.

Use **undo dns spoofing** to disable DNS spoofing.

Syntax

dns spoofing *ip-address*

undo dns spoofing *ip-address*

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address used to spoof DNS requests.

Usage guidelines

Use the **dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type A by responding with the specified IPv4 address.

The system allows only one replied IPv4 address for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing for the public network and specify IPv4 address 1.1.1.1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] dns spoofing 1.1.1.1
```

Related commands

dns proxy enable

dns trust-interface

Use **dns trust-interface** to specify a DNS trusted interface.

Use **undo dns trust-interface** to remove a DNS trusted interface.

Syntax

dns trust-interface *interface-type interface-number*

undo dns trust-interface [*interface-type interface-number*]

Default

No DNS trusted interface is specified.

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

By default, an interface obtains DNS suffix and DNS server information from DHCP. A network attacker might act as the DHCP server to assign a wrong DNS suffix and DNS server address to the device. As a result, the device fails to obtain the resolved IP address or might get the wrong IP

address. With the DNS trusted interface specified, the device only uses the DNS suffix and DNS server information obtained through the trusted interface to avoid attacks.

This configuration applies to both IPv4 DNS and IPv6 DNS.

You can configure a maximum of 128 DNS trusted interfaces on the device.

If you do not specify an interface, the **undo dns trust-interface** command removes all DNS trusted interfaces and restores the default.

Examples

Specify VLAN-interface 2 as a DNS trusted interface.

```
<Sysname> system-view
[Sysname] dns trust-interface vlan-interface 2
```

ip host

Use **ip host** to create a host name-to-IPv4 address mapping.

Use **undo ip host** to remove a host name-to-IPv4 address mapping.

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

Default

No host name-to-IPv4 address mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.).

ip-address: Specifies the IPv4 address of the host.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv4 address mappings for the public network.

For the public network, each host name maps to only one IPv4 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping** command parameter **ip**, **-a**, **-c**, **-f**, **-h**, **-i**, **-m**, **-n**, **-p**, **-q**, **-r**, **-s**, **-t**, **-tos**, or **-v** as the host name. For more information about the **ping** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv4 address 10.110.0.1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

Related commands

display dns host

ipv6 dns dscp

Use **ipv6 dns dscp** to set the DSCP value for IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Use **undo ipv6 dns dscp** to restore the default.

Syntax

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

Default

The DSCP value is 0 in IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing IPv6 DNS packets.

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

ipv6 dns server

Use **ipv6 dns server** to specify the IPv6 address of a DNS server.

Use **undo ipv6 dns server** to remove the IPv6 address of a DNS server.

Syntax

ipv6 dns server *ipv6-address* [*interface-type interface-number*]

undo ipv6 dns server [*ipv6-address* [*interface-type interface-number*]]

Default

No DNS server IPv6 address is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies the output interface by its type and number. If you do not specify an interface, the device forwards DNS packets out of the output interface of the matching route. Specify this argument if the IPv6 address of the DNS server is a link-local address. Do not specify this argument if the IPv6 address of the DNS server is a global unicast address.

Usage guidelines

For dynamic DNS, the device sends a DNS query request to the DNS servers in the order their IPv6 addresses are specified.

The system allows a maximum of six DNS server IPv6 addresses for the public network.

If you do not specify an IPv6 address, the **undo ipv6 dns server** command removes all DNS server IPv6 addresses for the public network.

Examples

Specify DNS server IPv6 address 2002::1 for the public network.

```
<Sysname> system-view
[Sysname] ipv6 dns server 2002::1
```

Related commands

display ipv6 dns server

ipv6 dns spoofing

Use **ipv6 dns spoofing** to enable DNS spoofing and specify the IPv6 address to spoof DNS requests.

Use **undo ipv6 dns spoofing** to disable DNS spoofing.

Syntax

ipv6 dns spoofing *ipv6-address*

undo ipv6 dns spoofing *ipv6-address*

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address used to spoof DNS requests.

Usage guidelines

Use the **ipv6 dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type AAAA by responding with the specified IPv6 address.

The system allows only one replied IPv6 address for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing for the public network and specify IPv6 address 2001::1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] ipv6 dns spoofing 2001::1
```

Related commands

dns proxy enable

ipv6 host

Use **ipv6 host** to create a host name-to-IPv6 address mapping.

Use **undo ipv6 host** to remove a host name-to-IPv6 address mapping.

Syntax

ipv6 host *host-name ipv6-address*

undo ipv6 host *host-name ipv6-address*

Default

No host name-to-IPv6 address mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6-address: Specifies the IPv6 address of the host.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv6 address mappings for the public network.

For the public network, each host name maps to only one IPv6 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping ipv6** command parameter **-a**, **-c**, **-i**, **-m**, **-q**, **-s**, **-t**, **-tc**, or **-v** as the host name. For more information about the **ping ipv6** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv6 address 2001::1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

Related commands

ip host

reset dns host

Use **reset dns host** to clear dynamic DNS entries.

Syntax

reset dns host [**ip** | **ipv6**]

Views

User view

Predefined user roles

network-admin

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, the **reset dns host** command clears dynamic DNS entries of all query types.

Examples

Clear dynamic DNS entries of all query types for the public network.

```
<Sysname> reset dns host
```

Related commands

display dns host

DDNS commands

The following compatibility matrixes show the support of hardware platforms for DDNS:

Hardware series	Model	Product code	DDNS compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	DDNS compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

ddns apply policy

Use **ddns apply policy** to apply a DDNS policy to an interface and enable DDNS update. DDNS updates the mapping between the FQDN and the primary IP address of the interface.

Use **undo ddns apply policy** to remove the application of a DDNS policy from an interface and to stop DDNS update.

Syntax

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy *policy-name*

Default

No DDNS policy and FQDN are specified on the interface, and DDNS update is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DDNS policy by its name, a case-insensitive string of 1 to 32 characters.

fqdn *domain-name*: Specifies the FQDN to replace <h> in the URL for DDNS update. The *domain-name* argument specifies a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

You can apply a maximum of four DDNS policies to an interface.

If you execute this command multiple times with the same DDNS policy name but different FQDNs, both of the following occur:

- The most recent configuration takes effect.
- The device initiates a DDNS update request immediately.

Examples

Apply DDNS policy **steven_policy** to VLAN-interface 2 to update the domain name-to-IP address mapping for FQDN **www.whatever.com** and enable DDNS update.

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

```
[Sysname-Vlan-interface2] ddns apply policy steven_policy fqdn www.whatever.com
```

Related commands

ddns policy

display ddns policy

ddns dscp

Use **ddns dscp** to set the DSCP value for outgoing DDNS packets.

Use **undo ddns dscp** to restore the default.

Syntax

ddns dscp *dscp-value*

undo ddns dscp

Default

The DSCP value for outgoing DDNS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DDNS packets.

```
<Sysname> system-view
[Sysname] ddns dscp 30
```

ddns policy

Use **ddns policy** to create a DDNS policy and enter its view, or enter the view of an existing DDNS policy.

Use **undo ddns policy** to delete a DDNS policy.

Syntax

ddns policy *policy-name*

undo ddns policy *policy-name*

Default

No DDNS policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the DDNS policy name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can create a maximum of 16 DDNS policies on the device.

Examples

Create a DDNS policy named **steven_policy** and enter its view.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
```

Related commands

ddns apply policy

display ddns policy

display ddns policy

Use **display ddns policy** to display information about DDNS policies.

Syntax

display ddns policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies a DDNS policy by its name, a case-insensitive string of 1 to 32 characters. If you do not specify a DDNS policy, this command displays information about all DDNS policies.

Examples

Display information about DDNS policy **steven_policy**.

```
<Sysname> display ddns policy steven_policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?
                     system=dyndns&hostname=<h>&myip=<a>
  Username         : steven
  Password         : ******
  Method           : GET
  SSL client policy:
  Interval         : 1 days 0 hours 1 minutes
```

Display information about all DDNS policies.

```
<Sysname> display ddns policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?system=
```

```
                    dyndns&hostname=<h>&myip=<a>
  Username          : steven
  Password          : ******
  Method            : GET
  SSL client policy:
  Interval          : 0 days 0 hours 30 minutes

DDNS policy: tom-policy
  URL               : http://members.3322.org/dyndns/update?system=
                      dyndns&hostname=<h>&myip=<a>
  Username          :
  Password          :
  Method            : GET
  SSL client policy:
  Interval          : 0 days 0 hours 15 minutes

DDNS policy: u-policy
  URL               : oray://phddns60.oray.net
  Username          : username
  Password          :
  Method            : -
  SSL client policy:
  Interval          : 0 days 0 hours 15 minutes
```

Table 5 Command output

Field	Description
DDNS policy	DDNS policy name.
URL	URL address for a DDNS update request. This field is empty if no URL address is configured.
Username	Username for logging in to the DDNS server. This field is empty if no username is configured.
Password	Password for logging in to the DDNS server. This field is empty if no password is configured and displays ********** if a password is configured.
Method	Parameter transmission method used to send HTTP/HTTPS-based DDNS update requests. Method types include GET and POST.
SSL client policy	Name of the associated SSL client policy. This field is empty if no SSL client policy is associated.
Interval	Interval for sending DDNS update requests.

Related commands

ddns policy

interval

Use **interval** to set the interval for sending DDNS update requests.

Use **undo interval** to restore the default.

Syntax

interval *days* [*hours* [*minutes*]]

undo interval

Default

The DDNS update request interval is one hour.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

days: Days in the range of 0 to 365.

hours: Hours in the range of 0 to 23.

minutes: Minutes in the range of 0 to 59.

Usage guidelines

Whether the interval is reached or not, a DDNS update request is initiated immediately if either of the following conditions occurs:

- The primary IP address of the interface changes.
- The link state of the interface changes from down to up.

If you set the interval to 0, the device does not periodically initiate DDNS update requests. However, it initiates a DDNS update request in either of the following situations:

- The primary IP address of the interface changes.
- The link state of the interface changes from down to up.

If you execute this command multiple times, the most recent configuration takes effect. If you change the interval for an applied DDNS policy, the device immediately initiates a DDNS update request and sets the interval as the update interval.

Examples

Set the interval to 1 day and 1 minute for sending DDNS update requests for DDNS policy **steven_policy**.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] interval 1 0 1
```

Related commands

ddns policy

display ddns policy

method

Use **method** to specify the parameter transmission method for sending DDNS update requests to HTTP/HTTPS-based DDNS servers.

Use **undo method** to restore the default.

Syntax

method { **http-get** | **http-post** }

undo method

Default

The method **http-get** applies.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

http-get: Uses the get operation.

http-post: Uses the post operation.

Usage guidelines

This command applies to DDNS updates in HTTP/HTTPS. If the DDNS server uses HTTP or HTTPS service, choose a parameter transmission method compatible with the DDNS server. For example, a DHS server supports the **http-post** method.

If the DDNS policy has been applied to an interface, a DDNS update is sent immediately after the parameter transmission is changed.

Examples

Specify the parameter transmission method as **http-post** for DDNS update requests for DDNS policy **steven_policy**.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] method http-post
```

Related commands

ddns policy

display ddns policy

password

Use **password** to specify the password for logging in to the DDNS server.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified for logging in to the DDNS server.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Examples

In DDNS policy **steven_policy**, specify **nevets** as the password for logging in to the DDNS server.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] password simple nevets
```

Related commands

ddns policy

display ddns policy

url

username

ssl-client-policy

Use **ssl-client-policy** to associate an SSL client policy with a DDNS policy.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy

Default

No SSL client policy is associated with a DDNS policy.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The SSL client policy is effective only for HTTPS-based DDNS update requests.

If you execute this command multiple times with different SSL client policies, the most recent configuration takes effect.

Examples

Associate SSL client policy **ssl_policy** with DDNS policy **steven_policy**.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] ssl-client-policy ssl_policy
```

Related commands

ddns policy

display ddns policy

ssl-client-policy (*Security Command Reference*)

url

Use **url** to specify the URL address for DDNS update requests.

Use **undo url** to restore the default.

Syntax

url *request-url*

undo url

Default

No URL address is specified for DDNS update requests.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

request-url: Specifies the URL address, a case-sensitive string of 1 to 240 characters.

Usage guidelines

The URL addresses configured for update requests vary by DDNS server. Common DDNS server URL address formats are shown in Table 6.

Table 6 Common URL addresses for DDNS update request

DDNS server	URL addresses for DDNS update requests
www.3322.org	http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
DYNDNS	http://members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
DYNS	http://www.dyns.cx/postscript.php?host=<h>&ip=<a>
ZONEEDIT	http://dynamic.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
TZO	http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>IPAddress=<a>
EASYDNS	http://members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&host_id=<h>
HEIPV6TB	http://dyn.dns.he.net/nic/update?hostname=<h>&myip=<a>
CHANGE-IP	http://nic.changeip.com/nic/update?hostname=<h>&offline=1
NO-IP	http://dynupdate.no-ip.com/nic/update?hostname=<h>&myip=<a>
DHS	http://members.dhs.org/nic/hosts?domain=dyn.dhs.org&hostname=<h>&hostscmd=edit&hostscmdstage=2&type=1&ip=<a>
HP	https://*server-name*/nic/update?group=*group-name*&myip=<a>
ODS	ods://update.ods.org
GNUDIP	gnudip://*server-name*
PeanutHull	• oray://phddns60.oray.net

DDNS server	URL addresses for DDNS update requests
	• oray://phservice2.oray.net

The URL address cannot contain the username or password. To configure the username and password, use the **username** command and the **password** command.

HP and GNUDIP are common DDNS update protocols. The *server-name* parameter is the domain name or IP address of the service provider's server using one of the update protocols.

The URL address for an update request can start with:

- **http://**—The HTTP-based DDNS server.
- **https://**—The HTTPS-based DDNS server.
- **ods://**—The TCP-based ODS server.
- **gnudip://**—The TCP-based GNUDIP server.
- **oray://**—The TCP-based DDNS server.

The domain names of DDNS servers are members.3322.org and phddns60.oray.net. The domain names of PeanutHull DDNS servers can be phddns60.oray.net and phservice2.oray.net. The domain name phservice2.oray.net maps to the public IP address of the old version PeanutHull DDNS server, which is not maintained any more. You need to try several times upon failures to connect to the server. As a best practice, register a new account and a domain name on the PeanutHull DDNS of a new version. Determine the domain name in the URL according to the actual situation.

The port number in the URL address is optional. If you do not specify a port number, the default port number is used. HTTP uses port 80, HTTPS uses port 443, and the PeanutHull server uses port 6060.

The system automatically performs the following tasks:

- Fills <h> with the FQDN that is specified when the DDNS policy is applied to an interface.
- Fills <a> with the primary IP address of the interface to which the DDNS policy is applied.

You can also manually specify an FQDN and an IP address in <h> and <a>, respectively. In this case, the FQDN that is specified when the DDNS policy is applied to an interface will not take effect. As a best practice, do not manually change the <h> and <a> because your configuration might be incorrect.

You cannot specify an FQDN and IP address in the URL address for contacting the PeanutHull server. Alternatively, you can specify an FQDN when applying the DDNS policy to an interface. The system automatically uses the primary IP address of the interface to which the DDNS policy is applied as the IP address for DDNS update.

To avoid misinterpretation, do not include colons (:), at signs (@), and question marks (?) in your login username or password, even if you can do so.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the URL address for DDNS update requests for DDNS policy **steven_policy**. The device contacts **www.3322.org** for DDNS update.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] url http://
members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
```

Related commands

ddns policy

display ddns policy

password

username

username

Use **username** to specify the username for logging in to the DDNS server.

Use **undo username** to restore the default.

Syntax

username *username*

undo username

Default

No username is specified for logging in to the DDNS server.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

username: Specifies the username, a case-sensitive string of 1 to 32 characters.

Examples

In DDNS policy **steven_policy**, specify **steven** as the username for logging in to the DDNS server.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] username steven
```

Related commands

ddns policy

display ddns policy

password

url

Contents

NAT commands 1

address 2
address interface 3
block-size 5
display nat address-group 5
display nat alg 7
display nat all 8
display nat dns-map 21
display nat eim 22
display nat inbound 23
display nat log 25
display nat no-pat 26
display nat outbound 28
display nat outbound port-block-group 30
display nat port-block 31
display nat port-block-group 33
display nat port-block-usage 35
display nat server 36
display nat server-group 38
display nat session 39
display nat static 42
display nat statistics 46
global-ip-pool 48
inside ip 49
local-ip-address 49
nat address-group 50
nat alg 51
nat dns-map 52
nat hairpin enable 53
nat icmp-error reply 54
nat inbound 55
nat inbound rule move 57
nat log alarm 57
nat log enable 58
nat log flow-active 59
nat log flow-begin 60
nat log flow-end 61
nat log port-block usage threshold 61
nat log port-block-assign 62
nat log port-block-withdraw 63
nat mapping-behavior endpoint-independent 63
nat outbound 64
nat outbound port-block-group 67
nat outbound rule move 68
nat port-block global-share enable 69
nat port-block-group 70
nat server 71
nat server rule move 75
nat server-group 76
nat static enable 77
nat static inbound 77
nat static inbound net-to-net 79
nat static inbound rule move 81
nat static outbound 82
nat static outbound net-to-net 83
nat static outbound rule move 85
nat timestamp delete 86

port-block ····87
port-range····88
reset nat count statistics····89
reset nat session····89

NAT commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

The following compatibility matrixes show the support of hardware platforms for NAT:

Hardware series	Model	Product code	NAT compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X • WX3024H • WX3024H-F No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	Yes

Hardware series	Model	Product code	NAT compatibility
	EWPXM1MAC0F	EWPXM1MAC0F	

Hardware series	Model	Product code	NAT compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

address

Use **address** to add an address range to a NAT address group.

Use **undo address** to remove an address range from a NAT address group.

Syntax

address *start-address end-address*

undo address *start-address end-address*

Default

No address ranges exist.

Views

NAT address group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start and end IP addresses of the address range. The end address must not be lower than the start address. If they are the same, the address range has only one IP address. You can specify a maximum of 65535 addresses in an IP address range.

Usage guidelines

A NAT address group is a set of address ranges. The source address in a packet destined for an external network is translated into an address in one of the address ranges.

Make sure the address ranges in a single NAT address group or in multiple NAT address groups do not overlap.

The **address** command and the **address interface** command are mutually exclusive for one NAT address group. Support for the **address interface** command varies by device model. For the command matrixes, see the **address interface** command.

Examples

Add address ranges to an address group.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
```

```
[Sysname-address-group-2] address 10.1.1.20 10.1.1.30
```

Related commands

address interface

nat address-group

address interface

Use **address interface** to add the IP address of an interface to a NAT address group.

Use **undo address interface** to restore the default.

Syntax

address interface *interface-type interface-number*

undo address interface

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: • WX2508H-PWR-LTE • WX2510H • WX2540H • WX2560H No: • WX2510H-F • WX2540H-F
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H	EWP-WX5540H	No

Hardware series	Model	Product code	Command compatibility
	WX5560H WX5580H	EWP-WX5560H EWP-WX5580H	
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Default

No interface address exists in a NAT address group.

Views

NAT address group view

Predefines user roles

network-admin

Parameters

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

Usage guidelines

This command is applicable to EasyIP with the IP address of the NAT interface dynamically obtained through DHCP or PPPoE. After you configure this command, the primary IPv4 address of the specified interface will be added to the NAT address group.

You can specify only one interface for a NAT address group.

The **address** command and the **address interface** command are mutually exclusive for one NAT address group.

The IP address of an interface cannot be added to different NAT address groups.

Make sure addresses in different NAT address groups do not overlap.

Examples

Add the IP address of VLAN-interface 20 to NAT address group **2**.

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

```
[Sysname] nat address-group 2
[Sysname-address-group-2] address interface vlan-interface20
```

Related commands

address

nat address-group

block-size

Use **block-size** to set the port block size.

Use **undo block-size** to restore the default.

Syntax

block-size *block-size*

undo block-size

Default

The port block size is 256.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

block-size: Specifies the number of ports for a port block. The value range for this argument is 1 to 65535.

Usage guidelines

Set an appropriate port block size based on the number of private IP addresses, the number of public IP addresses, and the port range in the port block group.

The port block size cannot be larger than the number of ports in the port range.

Examples

Set the port block size to 1024 for port block group **1**.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] block-size 1024
```

Related commands

nat port-block-group

display nat address-group

Use **display nat address-group** to display NAT address group information.

Syntax

display nat address-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535. If you do not specify the *group-id* argument, this command displays information about all NAT address groups.

Examples

Display information about all NAT address groups.

```
<Sysname> display nat address-group
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1    Address group name: a
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group ID: 2
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group ID: 3
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group ID: 4
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group ID: 6
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---
```

Display information about NAT address group **1**.

```
<Sysname> display nat address-group 1
  Address group ID: 1    Address group name: a
```

```
Port range: 1-65535
Address information:
  Start address         End address
  202.110.10.10         202.110.10.15
```

Table 1 Command output

Field	Description
NAT address group information	Information about the NAT address group
Address group ID	ID of the NAT address group.
Totally *n* NAT address groups	Total number of NAT address groups.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Port range	Port range for public IP addresses.
Port block size	Number of ports in a port block. This field is not displayed if the port block size is not set.
Extended block number	Number of extended port blocks. This field is not displayed if the number of extended port blocks is not set.
Address information	Information about the IP addresses in the address group. • For addresses added by using the **address** command: ○ **Start address**—Start IP address of an address range. If you do not specify a start address for the range, this field displays hyphens (**---**). ○ **End address**—End IP address of an address range. If you do not specify an end address for the range, this field displays hyphens (**---**). • For addresses added by using the **address interface** command: ○ **20.1.1.1 (Vlan-interface10)**—IP address 20.1.1.1 of VLAN-interface10 has been added to the NAT address group. ○ **--- (Vlan-interface10)**—Failed to add the IP address of VLAN-interface10 to the NAT address group because this interface does not have an IP address.

Related commands

nat address-group

display nat alg

Use **display nat alg** to display the NAT ALG status for all supported protocols.

Syntax

display nat alg

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the NAT ALG status for all supported protocols.

```
<Sysname> display nat alg
NAT ALG:
  DNS        : Enabled
  FTP        : Disabled
  H323       : Disabled
  ICMP-ERROR : Disabled
  ILS        : Disabled
  MGCP       : Disabled
  NBT        : Disabled
  PPTP       : Disabled
  RTSP       : Disabled
  RSH        : Disabled
  SCCP       : Disabled
  SIP        : Disabled
  SQLNET     : Disabled
  TFTP       : Disabled
  XDMCP      : Disabled
```

Related commands

`display nat all`

display nat all

Use **`display nat all`** to display all NAT configuration information.

Syntax

`display nat all`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display all NAT configuration information.

```
<Sysname> display nat all
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group ID: 2:
    Port range: 1-65535
```

```
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group ID: 3:
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group ID: 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group ID: 6:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---

NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
  2                   ---                   ---         ---
  3                   192.168.0.26          69          100

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y         NO-PAT:Y  Reversible: N
    Rule name: abc
    Priority: 1000
    NAT counting: 0
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
```

```
    Address group ID: 1
    Port-preserved: Y        NO-PAT: N  Reversible: N
    Rule name: lee
    Priority: 122
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: 1
    Port-preserved: N        NO-PAT: Y  Reversible: Y
    Rule name: rabbit
    Priority: 100
    NAT counting: 0
      The following items don't exist or aren't effective: ACL.

NAT internal server information:
  Totally 2 internal servers.
  Interface: Vlan-interface10
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : sept
    Priority      : 1000
    NAT counting  : 0
    Config status : Active

  Interface: Vlan-interface20
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    ACL           : 2000
    Rule name     : blue
    NAT counting  : 0
    Config status : Active

Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 2.2.2.1 – 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Rule name    : green
    Priority     : 4
    NAT counting : 0
```

```
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : blue
    Priority     : 4
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Rule name    : yellow
    Priority     : 5
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2001
    Reversible   : Y
    Rule name    : pink
    Priority     : 6
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

  Interface: Vlan-interface30
    Config status: Active

NAT DNS mappings:
  Totally 2 NAT DNS mappings.
```

```
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
  NO-PAT IP usage     : Disabled

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: Vlan-interface10
    Config status: Active

  Interface: Vlan-interface20
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS        : Enabled
  FTP        : Disabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RSH        : Enabled
  RTSP       : Enabled
```

```
  SCCP       : Enabled
  SIP        : Disabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---

NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    port-block-group: 2
    Rule name       : red
    NAT counting: 0
    Config status   : Active
```

```
  Interface: Vlan-interface20
    port-block-group: 10
    Rule name: lee
    NAT counting: 0
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.

Static NAT load balancing:     Disabled
```

(In IRF mode.) Display all NAT configuration information.

```
<Sysname> display nat all
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group 3:
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group 6:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---

NAT server group information:
```

```
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
  2                   ---                   ---         ---
  3                   192.168.0.26          69          100

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: Vlan-interface10
    ACL: 2038
    Address group ID: 2
    Add route: Y        NO-PAT: Y  Reversible: N
    Rule name: abcdefg
    Priority: 1000
    NAT counting : 0
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface20
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y        NO-PAT: N  Reversible: N
    Rule name: cdefg
    Priority: 1001
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: address group, and ACL.

  Interface: Vlan-interface20
    ACL: 2037
    Address group ID: 1
    Port-preserved: N        NO-PAT: Y  Reversible: Y
    Rule name: blue
    Priority: 1002
    NAT counting : 0
    Config status: Active.

NAT internal server information:
  Totally 5 internal servers.
  Interface: Vlan-interface10
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    NAT counting  : 0
```

```
    Config status : Active

  Interface: Vlan-interface20
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    ACL           : 2000
    Rule name     : green
    NAT counting  : 0
    Config status : Active

  Interface: Vlan-interface30
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Rule name     : blue
    NAT counting  : 0
    Config status : Active

  Interface: Vlan-interface40
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    ACL           : 3000
    Rule name     : white
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface50
    Protocol: 17(UDP)
    Global IP/port: 50.1.1.2/23
    Local IP/port : server group 1
                    192.168.0.26/23       (Connections: 10)
                    192.168.0.27/23       (Connections: 20)
    Rule name     : black
    NAT counting  : 0
    Config status : Active

Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 2.2.2.1 – 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
```

```
    Rule name     : pink
    Priority      : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : yellow
    Priority     : 1000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : grey
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2001
    Reversible   : Y
    Rule name    : orange
    Priority     : 10000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface40
    Config status: Active

  Interface: Vlan-interface50
    Config status: Active
```

```
NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
  NO-PAT IP usage     : Disabled

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: Vlan-interface40
    Config status: Active

  Interface: Vlan-interface50
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
```

```
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Disabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---

NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    port-block-group: 2
```

```
    Rule name: stone
    NAT counting: 0
    Config status   : Active

  Interface: Vlan-interface20
    port-block-group: 10
    NAT counting: 0
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.

Static NAT load balancing:     Disabled
```

The output shows all NAT configuration information. Table 2 describes only the fields for the output of the **nat hairpin enable**, **nat mapping-behavior**, and **nat alg** commands.

Table 2 Command output

Field	Description
NAT address group information	Information about the NAT address group. See Table 1 for output description.
NAT server group information	Information about the internal server group. See Table 14 for output description.
NAT inbound information:	Inbound dynamic NAT configuration. See Table 5 for output description.
NAT outbound information	Outbound dynamic NAT configuration. See Table 8 for output description.
NAT internal server information	NAT server mapping configuration. See Table 13 for output description.
Static NAT mappings	Static NAT mappings. See Table 16 for output description.
NAT DNS mappings	NAT DNS mappings. See Table 3 for output description.
NAT logging	NAT logging configuration. See Table 6 for output description.
NAT hairpinning	NAT hairpin configuration.
Interface	NAT hairpin-enabled interface.
Rule name	Name of the NAT rule.
NAT counting	Number of times the NAT rule is matched.
Priority	Priority of the NAT rule.
Config status	Status of the NAT hairpin configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT hairpin configuration does not take effect. This field is available when the **Config status** is **Inactive**.
NAT mapping behavior	Mapping behavior mode of PAT: **Endpoint-Independent** or **Address and Port-Dependent**.
ACL	ACL number or name. If no ACL is specified for NAT, this field displays hyphens (---).
Config status	Status of the NAT mapping behavior configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT mapping behavior configuration does not take

Field	Description
	effect. This field is available when the **Config status** is **Inactive**.
NAT ALG	NAT ALG configuration for different protocols.
NAT port block group information	Configuration information about NAT port block groups. See Table 11 for output description.
NAT outbound port block group information	Configuration information about static outbound port block mapping rules. See Table 9 for output description.

display nat dns-map

Use **display nat dns-map** to display NAT DNS mappings.

Syntax

display nat dns-map

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NAT DNS mappings.

```
<Sysname> display nat dns-map
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.
```

Table 3 Command output

Field	Description
NAT DNS mapping information	Information about NAT DNS mappings.
Totally *n* NAT DNS mappings	Total number of NAT DNS mappings.
Domain name	Domain name of the internal server.

Field	Description
Global IP	Public IP address of the internal server. • If Easy IP is configured, this field displays the IP address of the specified interface. • If you do not specify a public IP address, this field displays hyphens (**---**).
Global port	Public port number of the internal server.
Protocol	Protocol name and number of the internal server.
Config status	Status of the DNS mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the DNS mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat dns-map

display nat eim

Use **display nat eim** to display information about NAT Endpoint-Independent Mapping (EIM) entries.

Syntax

In standalone mode:

display nat eim

In IRF mode:

display nat eim [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays EIM entry information for all member devices. (In IRF mode.)

Usage guidelines

EIM entries are created when PAT operates in EIM mode. An EIM entry is a 3-tuple entry, and it records the mapping between a private address/port and a public address/port.

The EIM entry provides the following functions:

- The same EIM entry applies to subsequent connections initiated from the same source IP and port.
- The EIM entries allow reverse translation for connections initiated from external hosts to internal hosts.

Examples

(In standalone mode.) Display information about NAT EIM entries.

```
<Sysname> display nat eim
```

```
Slot 0:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

(In IRF mode.) Display information about EIM entries for the specified slot.

```
<Sysname> display nat eim slot 1
Slot 1:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

Table 4 Command output

Field	Description
Protocol	Protocol name and number.
Total entries found	Total number of EIM entries.

Related commands

nat mapping-behavior

nat outbound

display nat inbound

Use **display nat inbound** to display inbound dynamic NAT configuration.

Syntax

display nat inbound

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display inbound dynamic NAT configuration.

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y          NO-PAT: Y  Reversible: N
    Rule name: abcd
    Priority: 1000
    NAT counting: 0
    Config status: Active

Interface: Vlan-interface30
    ACL: 2037
    Address group ID: 1       Address group name: abc
    Add route: Y           NO-PAT: Y  Reversible: N
    Rule name: eif
    Priority: 1000
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
```

(In IRF mode.) Display inbound dynamic NAT configuration.

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y            NO-PAT: Y  Reversible: N
    Rule name: abcd
    Priority: 1000
    NAT counting: 0
    Config status: Active

Interface: Vlan-interface30
    Address group ID: 1
    Add route: Y             NO-PAT: Y  Reversible: N
    Rule name: eif
    Priority: 1001
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
```

Table 5 Command output

Field	Description
NAT inbound information	Information about inbound dynamic NAT configuration.

Field	Description
Totally *n* NAT inbound rules	Total number of inbound dynamic NAT rules.
Interface	Interface where the inbound dynamic NAT rule is configured.
ACL	ACL number or name.
Address group ID	ID of the NAT address group used by the inbound dynamic NAT rule.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Add route	Whether to add a route when a packet matches the inbound dynamic NAT rule: • **Y**—Adds a route. • **N**—Does not add a route.
NO-PAT	Whether NO-PAT or PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the inbound dynamic NAT rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the inbound dynamic NAT rule does not take effect: This field is available when the **Config status** is **Inactive**.

Related commands

`nat inbound`

display nat log

Use **`display nat log`** to display NAT logging configuration.

Syntax

`display nat log`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NAT logging configuration.

```
<Sysname> display nat log
NAT logging:
  Log enable          : Enabled(ACL 2000)
```

```
Flow-begin          : Disabled
Flow-end            : Disabled
Flow-active         : Enabled(10 minutes)
Port-block-assign   : Disabled
Port-block-withdraw : Disabled
Alarm               : Disabled
```

Table 6 Command output

Field	Description
NAT logging	NAT logging configuration.
Log enable	Enabling status of NAT logging. If an ACL is specified for NAT logging, this field also displays the ACL number or name.
Flow-begin	Enabling status of logging for NAT session establishment events.
Flow-end	Enabling status of logging for NAT session removal events.
Flow-active	Enabling status of logging for active NAT flows. If it is enabled, this field also displays the interval in minutes at which active flow logs are generated.
Port-block-assign	Enabling status of NAT444 user logging for port block assignment.
Port-block-withdraw	Enabling status of NAT444 user logging for port block withdrawal.
Alarm	Enabling status of logging for NAT alarms.

Related commands

`nat log enable`

`nat log flow-active`

`nat log flow-begin`

display nat no-pat

Use **`display nat no-pat`** command to display information about NAT NO-PAT entries.

Syntax

In standalone mode:

`display nat no-pat`

In IRF mode:

`display nat no-pat` [**`slot`** *`slot-number`*]

Views

Any view

Default user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NO-PAT entry information for all member devices. (In IRF mode.)

Usage guidelines

A NO-PAT entry records the mapping between a private address and a public address.

The NO-PAT entry provides the following functions:

- The same entry applies to subsequent connections initiated from the same source IP address.
- The NO-PAT entries allow reverse translation for connections initiated from external hosts to internal hosts.

Outbound and inbound NO-PAT address translations create their own NO-PAT tables. These two types of tables are displayed separately.

Examples

(In standalone mode.) Display information about NO-PAT entries for all cards.

```
<Sysname> display nat no-pat
Slot 0:
Global  IP: 200.100.1.100
Local   IP: 192.168.100.100
Reversible: N
Type      : Inbound
Local   IP: 192.168.100.200
Global  IP: 200.100.1.200
Reversible: Y
Type      : Outbound
Total entries found: 2
```

(In IRF mode.) Display information about NO-PAT entries for the specified slot.

```
<Sysname> display nat no-pat slot 1
Slot 1:
Global  IP: 200.100.1.100
Local   IP: 192.168.100.100
Reversible: N
Type      : Inbound
Local   IP: 192.168.100.200
Global  IP: 200.100.1.200
Reversible: Y
Type      : Outbound
Total entries found: 2
```

Table 7 Command output

Field	Description
Global IP	Public IP address.
Local IP	Private IP address.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.

Field	Description
Type	Type of the NO-PAT entry: • **Inbound**—A NO-PAT entry created during inbound dynamic NAT. • **Outbound**—A NO-PAT entry created during outbound dynamic NAT.
Total entries found	Total number of NO-PAT entries.

Related commands

nat inbound

nat outbound

display nat outbound

Use **display nat outbound** to display outbound dynamic NAT configuration.

Syntax

display nat outbound

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display outbound dynamic NAT configuration.

```
<Sysname> display nat outbound
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    Address group ID: 1
    Port-preserved: Y        NO-PAT: N  Reversible: N
    Rule name: acdefg
    Priority: 1000
    NAT counting: 0
    Config status: Active

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: ---
    Port-preserved: N         NO-PAT: Y  Reversible: Y
    Rule name: abefg
    Priority: 1000
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL
```

```
  Interface: Vlan-interface10
    ACL: 2100
    Address group ID: 2
    Port-preserved: N          NO-PAT: N  Reversible: N
    Priority: 0
    NAT counting: 0
    Config status: Active
```

(In IRF mode.) Display outbound dynamic NAT configuration.

```
<Sysname> display nat outbound
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y           NO-PAT: N  Reversible: N
    Rule name: abefg
    Priority: 1000
    NAT counting: 0
    Config status: Active

  Interface: Vlan-interface20
    ACL: 2037
    Address group ID: 2
    Port-preserved: N            NO-PAT: Y  Reversible: Y
    Rule name: cdefg
    Priority: 1001
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface10
    ACL: 2100
    Address group ID: 2
    Port-preserved: N             NO-PAT: N  Reversible: N
    Priority: 0
    NAT counting: 0
    Config status: Active
```

Table 8 Command output

Field	Description
NAT outbound information	Information about outbound dynamic NAT configuration.
Totally *n* NAT outbound rules	Total number of outbound dynamic NAT rules.
Interface	Interface where the outbound dynamic NAT rule is configured.
ACL	IPv4 ACL number or name. If no IPv4 ACL is specified for outbound dynamic NAT rule, this field displays hyphens (**---**).
Address group ID	ID of the address group used by the outbound dynamic NAT rule. If no

Field	Description
	address group is specified, the field displays hyphens (---).
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Port-preserved	Whether to try to preserve the port numbers for PAT. • **Y**—Tries to preserve the port numbers. • **N**—Allows translating port numbers.
NO-PAT	Whether NO-PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the outbound dynamic NAT rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the outbound dynamic NAT rule does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat outbound

display nat outbound port-block-group

Use **display nat outbound port-block-group** to display static outbound port block mapping rules for NAT444.

Syntax

display nat outbound port-block-group

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display static outbound port block mapping rules for NAT444.

```
<Sysname> display nat outbound port-block-group
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    port-block-group: 2
    Rule name: abcdefg
    NAT counting: 0
```

```
    Config status   : Active

  Interface: Vlan-interface20
    port-block-group: 10
    Rule name: abcfg
    NAT counting: 0
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

Table 9 Command output

Field	Description
NAT outbound port block group information	Information about static outbound port block mapping rules.
Totally *n* outbound port block group items	Total number of static outbound port block mapping rules.
Interface	Interface where the static outbound port block mapping rules configured.
port-block-group	ID of the port block group.
Rule name	Name of the static outbound port block mapping rule.
NAT counting	Number of times the mapping rule is matched.
Config status	Status of the port block mapping rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the port block mapping rule does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat outbound port-block-group

display nat port-block

Use **display nat port-block** to display NAT port block mappings.

Syntax

In standalone mode:

display nat port-block { **dynamic** [**address-group** { *group-id* | **name** *group-name* }] | **static** [**port-block-group** *group-id*] }

In IRF mode:

display nat port-block { **dynamic** [**address-group** { *group-id* | **name** *group-name* }] | **static** [**port-block-group** *group-id*] } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays dynamic port block mappings.

address-group: Displays port block mappings for the specified address group. If you do not specify a NAT address group, this command displays port block mappings for all address groups.

group-id: Specifies the ID of the address group. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the name of the address group. The name is a case-insensitive string of 1 to 63 characters.

static: Displays static port block mappings.

port-block-group *group-id*: Displays port block mappings for the specified port block group. The *group-id* argument specifies the ID of the port block group. The value range for the *group-id* argument is 0 to 65535. If you do not specify a port block group, this command displays port block mappings for all port block groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays port block mappings for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display static port block mappings.

```
<Sysname> display nat port-block static
Slot 0:
Local VPN     Local IP         Global IP        Port block   Connections
---           100.100.100.111  202.202.100.101  10001-10256  0
---           100.100.100.112  202.202.100.101  10257-10512  0
---           100.100.100.113  202.202.100.101  10513-10768  0
---           100.100.100.113  202.202.100.101  10769-11024  0
Total mappings found: 4
```

(In IRF mode.) Display static port block mappings for the specified slot.

```
<Sysname> display nat port-block static slot 1
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           100.100.100.111  202.202.100.101  10001-10256  0
---           100.100.100.112  202.202.100.101  10257-10512  0
---           100.100.100.113  202.202.100.101  10513-10768  0
---           100.100.100.113  202.202.100.101  10769-11024  0
Total mappings found: 4
```

(In standalone mode.) Display dynamic port block mappings.

```
<Sysname> display nat port-block dynamic
Slot 0:
Local VPN     Local IP         Global IP        Port block   Connections
---           101.1.1.12       192.168.135.201  10001-11024  1
Total mappings found: 1
```

(In IRF mode.) Display dynamic port block mappings.

```
<Sysname> display nat port-block dynamic slot 1
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           101.1.1.12       192.168.135.201  10001-11024  1
Total mappings found: 1
```

Table 10 Command output

Field	Description
Local VPN	This field is not supported in the current software version. MPLS L3VPN instance to which the private IP address belongs. If the private IP address does not belong to any VPN instance, this field displays hyphens (**---**).
Local IP	Private IP address.
Global IP	Public IP address.
Port block	Port block defined by a start port number and an end port number.
Connections	Number of connections established by using the ports in the port block.

display nat port-block-group

Use **display nat port-block-group** to display NAT port block group configuration.

Syntax

display nat port-block-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies the ID of a NAT port block group. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays configuration of all NAT port block groups.

Examples

Display configuration of all NAT port block groups.

```
<Sysname> display nat port-block-group
NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
```

```
  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---
```

Display information about NAT port block group **1**.

```
<Sysname> display nat port-block-group 1
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
```

Table 11 Command output

Field	Description
NAT port block group information	Information about the port block group configuration.
Totally *n* NAT port block groups	Total number of port block groups.
Port block group	ID of the port block group.
Port range	Port range for the public IP addresses.
Block size	Number of ports in a port block.
Local IP address information	Information about the private IP addresses.
Global IP pool information	Information about the public IP addresses.
Start address	Start IP address of a private or public IP address range. If no start IP address is specified for the address range, this field displays hyphens (**---**).

Field	Description
End address	End IP address of a private or public IP address range. If no end IP address is specified for the address range, this field displays hyphens (**---**).
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance to which the private IP address range belongs. If no VPN instance is specified for the private address range, this field displays hyphens (**---**).

Related commands

nat port-block-group

display nat port-block-usage

Use **display nat port-block-usage** to display the port block usage for address groups.

Syntax

In standalone mode:

display nat port-block-usage [**address-group** *group-id*]

In IRF mode:

display nat port-block-usage [**address-group** *group-id*] [**slot** *slot-number*]

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

address-group *group-id*: Specifies the ID of an address group. The value range for the *group-id* argument is 0 to 65535. If you do not specify an address group, this command displays the port block usage for all address groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the port block usage for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display the port block usage for address groups.

```
<Sysname> display nat port-block-usage
Slot 1:
Address group 0 on channel 0:
  Total port block entries :10
  Active port block entries:9
  Current port block usage :90%

Total NAT address groups found: 1
```

(In IRF mode.) Display the port block usage for address groups for slot 1.

```
<Sysname> display nat port-block-usage slot 1
```

```
Slot 1:
Address group 0 on channel 0:
  Total port block entries :10
  Active port block entries:9
  Current port block usage :90%
Total NAT address groups found: 1
```

Table 12 Command output

Field	Description
CPU	Number of the CPU.
Address group	ID of the address group.
channel	Field-programmable gate array (FPGA) ID.
Total port block entries	Total number of port blocks in the address group.
Active port block entries	Total number of assigned port blocks in the address group.
Current port block usage	Port block usage in the address group.
Total NAT address groups found	Total number of address groups.

display nat server

Use **display nat server** to display NAT server mappings.

Syntax

display nat server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display NAT server mappings.

```
<Sysname> display nat server
NAT internal server information:
  Totally 2 internal servers.
  Interface: Vlan-interface10
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Rule name     : abcg
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface20
```

```
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Rule name     : abcdefg
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: interface IP address.
```

(In IRF mode.) Display NAT server mappings.

```
<Sysname> display nat server

NAT internal server information:
  Totally 5 internal servers.
  Interface: Vlan-interface10
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    NAT counting  : 0
    Config status : Active

  Interface: Vlan-interface30
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    Rule name     : ace
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:

  Interface: Vlan-interface40
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Rule name     : abcdef
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface40
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Rule name     : cdefg
    NAT counting  : 0
    Config status : Active
```

```
Interface: Vlan-interface50
  Protocol: 17(UDP)
  Global IP/port: 50.1.1.2/23
  Local IP/port : server group 1
                  1.1.1.1/21            (Connections: 10)
                  192.168.100.200/80    (Connections: 20)
  Rule name     : white
  NAT counting  : 0
  Config status : Active
```

Table 13 Command output

Field	Description
NAT internal server information	Information about NAT server mapping.
Interface	Interface where the NAT server mapping is configured.
Protocol	Protocol number and name of the internal server.
Global IP/port	Public IP address and port number of the internal server. • **Global IP**—A single IP address or an IP address range. If you use Easy IP, this field displays the IP address of the specified interface. If you do not specify an address for the interface, the **Global IP** field displays hyphens (**---**). • **port**—A single port number or a port number range. If no port number is in the specified protocol, the **port** field displays hyphens (**---**).
Local IP/port	For common NAT server mappings and object group-based NAT server mappings, this field displays the private IP address and port number of the internal server. • **Local IP**—A single IP address or an IP address range. • **port**—A single port number or a port number range. If no port number is in the specified protocol, the **port** field displays hyphens (---). For a load sharing NAT server mapping, this field displays the internal server group ID, IP address, port number, and number of connections of each member.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Rule name	Name of the NAT server mapping.
NAT counting	Number of times the NAT server mapping is matched.
Config status	Status of the NAT server mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT server mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat server

display nat server-group

Use **display nat server-group** to display internal server group configuration.

Syntax

display nat server-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies the ID of the internal server group. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays the configuration of all internal server groups.

Examples

Display the configuration of all internal server groups.

```
<Sysname> display nat server-group
NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP            Port        Weight
  1                   192.168.0.26         23          100
                      192.168.0.27         23          500
  2                   ---                  ---         ---
  3                   192.168.0.26         69          100
```

Display the configuration of internal server group **1**.

```
<Sysname> display nat server-group 1
  Group Number        Inside IP            Port        Weight
  1                   192.168.0.26         23          100
                      192.168.0.27         23          500
```

Table 14 Command output

Field	Description
NAT server group information	Information about the NAT server group configuration.
Totally *n* NAT server groups	Total number of NAT server groups.
Group Number	ID of the internal server group.
Inside IP	Private IP address of a server in the internal server group. If no address is specified, this field displays hyphens (---).
Port	Private port number of a server in the internal server group. If no port number is specified, this field displays hyphens (**---**).
Weight	Weight of a server in the internal server group. If no weight value is specified, this field displays hyphens (**---**).

Related commands

nat server-group

display nat session

Use **display nat session** to display NAT sessions.

Syntax

In standalone mode:

display nat session [[**responder**] { **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**verbose**]

In IRF mode:

display nat session [[**responder**] { **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

responder: Displays NAT sessions by responder. If you do not specify this keyword, this command displays NAT sessions by initiator.

source-ip *source-ip*: Displays NAT sessions for the source IP address specified by the *source-ip* argument. The IP address must be the source IP address of the packet that triggers the session establishment.

destination-ip *destination-ip*: Displays NAT sessions for the destination IP address specified by the *destination-ip* argument. The IP address must be the destination IP address of the packet that triggers the session establishment.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT sessions for all member devices. (In IRF mode.)

verbose: Displays detailed information about NAT sessions. If you do not specify this keyword, this command displays brief information about NAT sessions.

Usage guidelines

If you do not specify any parameters, this command displays all NAT sessions.

Examples

(In standalone mode.) Display detailed information about NAT sessions.

```
<Sysname> display nat session verbose
Slot 0:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
```

```
  Protocol: TCP(6)
  Inbound interface: Vlan-interface20
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Rule ID: -/-/-
Rule name:
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

(In IRF mode.) Display detailed information about NAT sessions for the specified slot.

```
<Sysname> display nat session slot 1 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface20
State: TCP_SYN_SENT
Application: SSH
Rule ID: -/-/-
Rule name:
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

Table 15 Command output

Field	Description
Initiator	Session information about the initiator.
Responder	Session information about the responder.
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
DS-Lite tunnel peer	Destination address of the DS-Lite tunnel interface. If the session does not

Field	Description
	belong to any DS-Lite tunnel, this field displays a hyphen (**-**).
VPN instance/VLAN ID/Inline ID	The fields identify the following information: • **VPN instance**—MPLS L3VPN instance to which the session belongs. The **VPN instance** field is not supported in the current software version. • **VLAN ID**—VLAN ID to which the session belongs for Layer 2 forwarding. • **Inline ID**—INLINE to which the session belongs for Layer 2 forwarding. If no VPN instance, VLAN ID, or inline ID is specified, a hyphen (-) is displayed for the related field.
Protocol	Transport layer protocol type: **DCCP**, **ICMP**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.
Inbound interface	Input interface.
State	NAT session status.
Application	Application layer protocol type, such as **FTP** and **DNS**. This field displays **OTHER** for the protocol types identified by non-well-known ports.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Time when the session starts.
TTL	Remaining NAT session lifetime in seconds.
Initiator->Responder	Number of packets and packet bytes from the initiator to the responder.
Responder->Initiator	Number of packets and packet bytes from the responder to the initiator.
Total sessions found	Total number of sessions.

Related commands

`reset nat session`

display nat static

Use **`display nat static`** to display static NAT mappings.

Syntax

`display nat static`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

(In standalone mode.) Display static NAT mappings.

```
<Sysname> display nat static
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
```

```
  Net-to-net:
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    NAT counting : 0
    Rule name    : abcdefg
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
   Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN, and ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2001
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
```

```
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

  Interface: Vlan-interface30
    Config status: Active
```

(In IRF mode.) Display static NAT mappings.

```
<Sysname> display nat static
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : adefg
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Global IP   : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
```

```
    ACL:         : 2000
    Rule name    : defg
    Priority     : 1000
    NAT counting : 0
    Reversible   : Y
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active
```

Table 16 Command output

Field	Description
Static NAT mappings	Information about static NAT mapping configuration.
Totally *n* inbound static NAT mappings	Total number of inbound static NAT mappings.
Totally *n* outbound static NAT mappings	Total number of outbound static NAT mappings.
Net-to-net	Net-to-net static NAT mapping.
IP-to-IP	One-to-one static NAT mapping.
Local IP	Private IP address or address range.
Global IP	Public IP address or address range.
Netmask	Network mask.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Reversible	Whether reverse address translation is allowed. If reverse address translation is allowed, this field displays **Y**. If reverse address translation is not allowed, this field is not displayed.
Interfaces enabled with static NAT	Interfaces on which static NAT is enabled.
Totally *n* interfaces enabled with static NAT	Total number of interfaces where static NAT is enabled.
Interface	Interface on which static NAT is enabled.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the static NAT mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the static NAT mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat static enable

nat static inbound

nat static inbound net-to-net

nat static outbound

nat static outbound net-to-net

display nat statistics

Use **display nat statistics** to display NAT statistics.

Syntax

In standalone mode:

display nat statistics [**summary**]

In IRF mode:

display nat statistics [**summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays NAT statistics summary. If you do not specify this keyword, this command displays detailed NAT statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT statistics for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display detailed information about NAT statistics.

```
<Sysname> display nat statistics
Slot 0:
  Session creation rate: 0
  Total session entries: 100
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

(In IRF mode.) Display detailed information about NAT statistics.

```
<Sysname> display nat statistics
Slot 1:
  Total session entries: 100
  Session creation rate: 0
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
```

```
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

Table 17 Command output

Field	Description
Total session entries	Number of NAT session entries.
Session creation rate	Number of NAT sessions created per second.
Total EIM entries	Total number of EIM entries.
Total inbound NO-PAT entries	Total number of inbound NO-PAT entries.
Total outbound NO-PAT entries	Total number of outbound NO-PAT entries.
Total static port block entries	Total number of static NAT444 mappings.
Total dynamic port block entries	Total number of dynamic port block mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
Active static port block entries	Number of static port block mappings that are in use.
Active dynamic port block entries	Number of dynamic port block mappings that have been created. It equals the number of dynamically assigned port blocks.

(In standalone mode.) Display NAT statistics summary.

```
<Sysname> display nat statistics summary
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM       SPB       DPB       ASPB      ADPB
0    100       1         10        15        0         0
```

(In IRF mode.) Display NAT statistics summary.

```
<Sysname> display nat statistics summary
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM       SPB       DPB       ASPB      ADPB
2    0         0         0         1572720   0         0
```

Table 18 Command output

Field	Description
Sessions	Number of NAT session entries.

Field	Description
EIM	Number of EIM entries.
SPB	Number of static NAT444 mappings.
DPB	Number of dynamic port block mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
ASPB	Number of static port block mappings in use.
ADPB	Number of dynamic port block mappings that have been created. It equals the number of dynamically assigned port blocks.

global-ip-pool

Use **global-ip-pool** to add a public IP address range to a NAT port block group.

Use **undo global-ip-pool** to remove a public IP address range from a NAT port block group.

Syntax

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address* [*end-address*]

Default

No public IP address ranges exist.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a public IP address range. The end IP address cannot be lower than the start IP address. If the start and end IP addresses are the same, only one public IP address is specified.

Usage guidelines

A static port block mapping maps a public IP address to multiple private IP addresses and assigns a unique port block to each private IP address. The number of port blocks that a public IP address can assign is determined by dividing the number of ports in the port range by the port block size.

Every time you execute this command, an address range can contain a maximum of 255 public IP addresses. All public IP address ranges in one port block group cannot overlap.

Public IP address ranges in different port block groups can overlap. The port ranges for overlapped public IP address ranges cannot overlap.

Examples

Add a public IP address range to the port block group **1**. The public IP address range consists of IP addresses from 202.10.1.1 to 202.10.1.10.

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

```
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10
```

Related commands

nat port-block-group

inside ip

Use **inside ip** to add a server to an internal server group.

Use **undo inside ip** to remove a server from an internal server group.

Syntax

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

Default

An internal server group has no server members.

Views

Internal server group view

Predefined user roles

network-admin

Parameters

inside-ip: Specifies the IP address of an internal server.

port *port-number*: Specifies the port number of an internal server, in the range of 1 to 65535, excluding FTP port 20.

weight *weight-value*: Specifies the weight of the internal server. The value range is 1 to 1000, and the default value is 100.

Usage guidelines

An internal server with a larger weight receives a larger percentage of connections in the internal server group.

Examples

Add a server with IP address 10.1.1.2 and port number 30 to internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
[Sysname-nat-server-group-1] inside ip 10.1.1.2 port 30
```

Related commands

nat server-group

local-ip-address

Use **local-ip-address** to add a private IP address range to a NAT port block group.

Use **undo local-ip-address** to remove a private IP address range from a NAT port block group.

Syntax

local-ip-address *start-address end-address*

undo local-ip-address *start-address* [*end-address*]

Default

No private IP address ranges exist in a NAT port block group.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a private IP address range. The end IP address cannot be lower than the start IP address. If the start and end IP addresses are the same, only one private IP address is specified.

Usage guidelines

A static port block mapping maps one public IP address to multiple private IP addresses and assigns a unique port block to each private IP address.

In a NAT port block group, the number of private IP addresses cannot be larger than the number of assignable port blocks. Otherwise, some private IP addresses cannot obtain port blocks. The number of port blocks that a public IP address can assign is determined by dividing the number of ports in the port range by the port block size.

Examples

Add a private IP address range to port block group 1. The private IP address range consists of IP addresses from 172.16.1.1 to 172.16.1.255.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255
```

Related commands

nat port-block-group

nat address-group

Use **nat address-group** to create a NAT address group and enter its view, or enter the view of an existing NAT address group.

Use **undo nat address-group** to delete a NAT address group.

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

Default

No NAT address groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535.

name *group-name*: Assigns a name to the NAT address group. The *group-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

A NAT address group is a set of address ranges. Use the **address** command to add an address range to a NAT address group. Dynamic NAT translates the source IP address of a packet into an IP address in the address group.

Examples

Create a NAT address group numbered 1 and named **abc**.

```
<Sysname> system-view
[Sysname] nat address-group 1 name abc
```

Related commands

address

display nat address-group

display nat all

nat inbound

nat outbound

nat alg

Use **nat alg** to enable NAT ALG for the specified or all supported protocols.

Use **undo nat alg** to disable NAT ALG for the specified or all supported protocols.

Syntax

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

Default

NAT ALG is enabled for DNS, FTP, ICMP error messages, RTSP, and PPTP, and is disabled for the other supported protocols.

Views

System view

Predefined user roles

network-admin

Parameters

all: Enables NAT ALG for all supported protocols.

dns: Enables NAT ALG for DNS.

ftp: Enables NAT ALG for FTP.

h323: Enables NAT ALG for H.323.

icmp-error: Enables NAT ALG for ICMP error packets.

ils: Enables NAT ALG for ILS.

mgcp: Enables NAT ALG for MGCP.

nbt: Enables NAT ALG for NBT.

pptp: Enables NAT ALG for PPTP.

rsh: Enables NAT ALG for RSH.

rtsp: Enables NAT ALG for RTSP.

sccp: Enables NAT ALG for SCCP.

sip: Enables NAT ALG for SIP.

sqlnet: Enables NAT ALG for SQLNET.

tftp: Enables NAT ALG for TFTP.

xdmcp: Enables NAT ALG for XDMCP.

Usage guidelines

NAT ALG translates address or port information in the application layer payload to ensure connection establishment.

For example, an FTP application includes a data connection and a control connection. The IP address and port number for the data connection depend on the payload information of the control connection. This requires NAT ALG to translate the address and port information to establish the data connection.

Examples

Enable NAT ALG for FTP.

```
<Sysname> system-view
[Sysname] nat alg ftp
```

Related commands

display nat all

nat dns-map

Use **nat dns-map** to configure a NAT DNS mapping.

Use **undo nat dns-map** to remove a NAT DNS mapping.

Syntax

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

Default

No NAT DNS mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

domain *domain-name*: Specifies the domain name of an internal server. A domain name is a dot-separated case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.) (for example, aabbcc.com). The domain name can contain a maximum of 253 characters, and each separated string contains no more than 63 characters.

protocol *pro*-type: Specifies the type of the protocol used by the internal server, **tcp** or **udp**.

interface *interface-type interface-number*: Enables Easy IP to use the IP address of the interface specified by its type and number as the public address of the internal server.

ip *global-ip*: Specifies the public IP address used by the internal server to provide services for the external network.

port *global-port*: Specifies the public port number used by the internal server to provide services for the external network. The port number format can be one of the following:

- A number in the range of 1 to 65535.
- A protocol name, a string of 1 to 15 characters. For example, **ftp** and **telnet**.

Usage guidelines

NAT DNS mapping must cooperate with the NAT Server feature.

- A NAT DNS mapping maps the domain name of an internal server to the public IP address, public port number, and protocol type of the internal server.
- A NAT server mapping maps the public IP and port to the private IP and port of the internal server.

The cooperation allows an internal host to access an internal server on the same private network by using the domain name of the internal server when the DNS server is on the public network. The DNS reply from the external DNS server contains only the domain name and public IP address of the internal server in the payload. The NAT interface might have multiple internal servers configured with the same public IP address but different private IP addresses. DNS ALG might find an incorrect internal server by using only the public IP address. If a DNS mapping is configured, DNS ALG can obtain the public IP address, public port number, and protocol type of the internal server by using the domain name. Then it can find the correct internal server by using the public IP address, public port number, and protocol type of the internal server.

You can configure multiple NAT DNS mappings.

Examples

Configure a NAT DNS mapping to map the domain name **www.server.com** to the public IP address **202.112.0.1**, public port number **12345**, and protocol type TCP.

```
<Sysname> system-view
[Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345
```

Related commands

display nat all

display nat dns-map

nat server

nat hairpin enable

Use **nat hairpin enable** to enable NAT hairpin.

Use **undo nat hairpin enable** to disable NAT hairpin.

Syntax

nat hairpin enable

undo nat hairpin enable

Default

NAT hairpin is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

NAT hairpin allows internal hosts to access each other or allows internal hosts to access internal servers. It must cooperate with NAT Server, outbound dynamic NAT, or outbound static NAT. The source and destination IP addresses of the packets are translated on the interface connected to the internal network.

Examples

Enable NAT hairpin on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat hairpin enable
```

Related commands

display nat all

nat icmp-error reply

Use **nat icmp-error reply** to enable sending ICMP error messages upon NAT failures.

Use **undo nat icmp-error reply** to restore the default.

Syntax

nat icmp-error reply

undo nat icmp-error reply

Default

No ICMP error messages are sent upon NAT failures.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Disabling sending ICMP error messages upon NAT failures reduces useless packets, saves bandwidth, and avoids exposing the device IP address to the public network.

This command is required for traceroute.

Examples

Enable sending ICMP error messages upon NAT failures.

```
<Sysname> system-view
[Sysname] nat icmp-error reply
```

nat inbound

Use **nat inbound** to configure an inbound dynamic NAT rule.

Use **undo nat inbound** to delete an inbound dynamic NAT rule.

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

Default

No inbound dynamic NAT rules exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

address-group *group-id*: Specifies an address group for address translation.

group-id: Specifies the address group ID. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the address group name, a case-insensitive string of 1 to 63 characters.

no-pat: Uses the NO-PAT mode. If you do not specify this keyword, PAT is used. PAT supports only TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Enables reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the internal network to the external network.

add-route: Automatically adds a route to the source address after translation. The output interface is the NAT interface and the next hop is the source address before translation.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

priority *priority*: Specifies a priority for the rule, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the rule has the lowest priority among the same type of NAT rules.

disable: Disables the inbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

description *text*: Specifies a description for the inbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Inbound dynamic NAT translates the source IP addresses of incoming packets permitted by the ACL into IP addresses in the address group.

Inbound dynamic NAT supports the following modes:

- **PAT**—Performs both IP address translation and port translation.
- **NO-PAT**—Performs only IP address translation.

The NO-PAT mode supports reverse address translation. Reverse address translation uses ACL reverse matching to identify packets to be translated. ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Inbound dynamic NAT typically cooperates with one of the following to implement bidirectional NAT:

- Outbound dynamic NAT (the **nat outbound** command).
- NAT Server (the **nat server** command).
- Outbound static NAT (the **nat static** command).

An address group cannot be used by both the **nat inbound** and **nat outbound** commands. It cannot be used by the **nat inbound** command in both PAT and NO-PAT modes.

Do not specify the **add-route** keyword if the subnets where the internal and external networks reside overlap. For other network scenarios:

- If you specify the **add-route** keyword, the device automatically adds a route to the source address after translation for a packet. The destination address is the NATed address in the NAT address group, the output interface is the interface where the command is executed, and the next hop is the source address before translation.
- If you do not specify the **add-route** keyword, you must manually add the route. As a best practice, add routes manually because automatic route adding is slow.

An ACL can be used by only one inbound dynamic NAT rule on an interface.

You can configure multiple inbound dynamic NAT rules on an interface.

Inbound dynamic NAT rules configured with the same priority value are matched by using their ACLs.

- NAT rules with named ACLs have higher priorities than NAT rules with unnamed ACLs.
- NAT rules with named ACLs are matched in alphabetical order of their ACL names.
- NAT rules with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure ACL 2001 to permit packets only from subnet 10.110.10.0/24 to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Create address group 1 and add the address range of 202.110.10.10 to 202.110.10.12 to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an inbound NO-PAT rule on interface VLAN-interface 10. NAT translates the source addresses of incoming packets into the addresses in address group 1, and automatically adds routes for translated packets. Set the rule name to **abc**, and the priority to 0.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0
```

Related commands

display nat all

display nat inbound

display nat no-pat

nat inbound rule move

Use **nat inbound rule move** to change the priority of an inbound dynamic NAT rule.

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of the rule be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named inbound dynamic NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the inbound dynamic NAT rule **abc** to the line before the rule **def**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat inbound rule move abc before def
```

Related commands

nat inbound

nat log alarm

Use **nat log alarm** to enable NAT alarm logging.

Use **undo nat log alarm** to disable NAT alarm logging.

Syntax

nat log alarm

undo nat log alarm

Default

NAT alarm logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Packets that need to be translated are dropped if the NAT resources are not enough. In NO-PAT, the NAT resources refer to the public IP addresses. In EIM PAT, the NAT resources refer to public IP addresses and ports. In NAT444, the NAT resources refer to public IP addresses, port blocks, or ports in port blocks. NAT alarm logging monitors the usage of NAT resources and outputs logs if the NAT resources are not enough.

The NAT444 gateway generates alarm logs when the ports in the extended port blocks of a dynamic port block mapping are all occupied.

Before configuring alarm logging for NAT, you must configure the custom NAT log generation and outputting features. For more information about information center, see *System Management Configuration Guide*.

This command take effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT alarm logging.

```
<Sysname> system-view
[Sysname] nat log alarm
```

Related commands

display nat all

display nat log

nat log enable

nat log enable

Use **nat log enable** to enable NAT logging.

Use **undo nat log enable** to disable NAT logging.

Syntax

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

Default

NAT logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

acl: Specifies an ACL.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

You must enable NAT logging before you enable NAT session logging, NAT444 user logging (including port block assignment and withdrawal logging), NAT alarm logging, or NAT NO-PAT logging.

The **acl** keyword takes effect only for NAT session logging. If an ACL is specified, flows matching the permit rule might trigger NAT session logs. If you do not specify an ACL, all flows processed by NAT might trigger NAT session logs.

Examples

Enable NAT logging.

```
<Sysname> system-view
[Sysname] nat log enable
```

Related commands

display nat all

display nat log

nat log alarm

nat log flow-active

nat log flow-begin

nat log flow-end

- **nat log port-block-assign**
- **nat log port-block-withdraw**

nat log flow-active

Use **nat log flow-active** to enable logging for active NAT flows and set the logging interval.

Use **undo nat log flow-active** to disable logging for active NAT flows.

Syntax

nat log flow-active *time-value*

undo nat log flow-active

Default

Logging for active NAT flows is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the interval for logging active NAT flows, in the range of 10 to 120 minutes.

Usage guidelines

Active NAT flows are NAT sessions that last for a long time. The logging feature helps track active NAT flows by periodically logging the active NAT flows.

Logging for active NAT flows takes effect only after you enable NAT logging.

Examples

Enable logging for active NAT flows and set the logging interval to 10 minutes.

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

Related commands

display nat all

display nat log

nat log enable

nat log flow-begin

Use **nat log flow-begin** to enable logging for NAT session establishment events.

Use **undo nat log flow-begin** to disable logging for NAT session establishment events.

Syntax

nat log flow-begin

undo nat log flow-begin

Default

Logging for NAT session establishment events is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Logging for NAT session establishment events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session establishment events.

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

Related commands

display nat all

display nat log

nat log enable

nat log flow-end

Use **nat log flow-end** to enable logging for NAT session removal events.

Use **undo nat log flow-end** to disable logging for NAT session removal events.

Syntax

nat log flow-end

undo nat log flow-end

Default

Logging for NAT session removal events is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Logging for NAT session removal events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session removal events.

```
<Sysname> system-view
[Sysname] nat log flow-end
```

Related commands

display nat all

display nat log

nat log enable

nat log port-block usage threshold

Use **nat log port-block usage threshold** to set the port block usage threshold.

Use **undo nat log port-block port-usage threshold** to restore the default.

Syntax

nat log port-block usage threshold *value*

undo nat log port-block usage threshold

Default

The port block usage threshold is 90%.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies a threshold in the range of 40 to 100 in percentage.

Usage guidelines

A log is generated when the port block usage exceeds the threshold.

Examples

Set the port block usage threshold to 60%.

```
<Sysname> system-view
[Sysname] nat log port-block usage threshold 60
```

Related commands

display nat all

display nat log

nat log enable

nat log port-block-assign

Use **nat log port-block-assign** to enable NAT444 user logging for port block assignment.

Use **undo nat log port-block-assign** to disable NAT444 user logging for port block assignment.

Syntax

nat log port-block-assign

undo nat log port-block-assign

Default

NAT444 user logging is disabled for port block assignment.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For static port block mappings, the NAT444 gateway generates a user log when it translates the first connection from a private IP address.

For dynamic port block mappings, the NAT444 gateway generates a user log when it assigns or extends a port block for a private IP address.

This command takes effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT444 user logging for port block assignment.

```
<Sysname> system-view
[Sysname] nat log port-block-assign
```

Related commands

display nat all

display nat log

nat log enable

nat log port-block-withdraw

Use **nat log port-block-withdraw** to enable NAT444 user logging for port block withdrawal.

Use **undo nat log port-block-withdraw** to disable NAT444 user logging for port block withdrawal.

Syntax

nat log port-block-withdraw

undo nat log port-block-withdraw

Default

NAT444 user logging is disabled for port block withdrawal.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For static port block mappings, the NAT444 gateway generates a user log when all connections from a private IP address are disconnected.

For dynamic port block mappings, the NAT444 gateway generates a user log when all the following conditions are met:

- The port blocks (including the extended ones) assigned to the private IP address are withdrawn.
- The corresponding mapping entry is deleted.

This command takes effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT444 user logging for port block withdrawal.

```
<Sysname> system-view
[Sysname] nat log port-block-withdraw
```

Related commands

display nat all

display nat log

nat log enable

nat mapping-behavior endpoint-independent

Use **nat mapping-behavior endpoint-independent** to specify the Endpoint-Independent Mapping (EIM) mode for PAT.

Use **undo nat mapping-behavior** to restore the default.

Syntax

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

Default

Address and Port-Dependent Mapping applies.

Views

System view

Predefined user roles

network-admin

Parameters

acl: Specifies an ACL to define the applicable scope of Endpoint-Independent Mapping.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

PAT supports the following NAT mapping modes:

- **Endpoint-Independent Mapping**—Uses the same IP and port mapping (EIM entry) for packets from the same source and port to any destination. EIM allows external hosts to access the internal hosts by using the translated IP address and port. It allows internal hosts behind different NAT gateways to access each other.
- **Address and Port-Dependent Mapping**—Uses different IP and port mappings for packets with the same source IP and port to different destination IP addresses and ports. APDM allows an external host to access an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.

This command takes effect only on outbound PAT. Address and Port-Dependent Mapping always applies to inbound PAT.

If you specify an ACL, Endpoint-Independent Mapping applies to packets that are permitted by the ACL. If you do not specify an ACL, Endpoint-Independent Mapping applies to all packets.

Examples

Apply the Endpoint-Independent Mapping mode to all packets for address translation.

```
<Sysname> system-view
[Sysname] nat mapping-behavior endpoint-independent
```

Apply the Endpoint-Independent Mapping mode to FTP and HTTP packets, and the Address and Port-Dependent Mapping mode to other packets for address translation.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] nat mapping-behavior endpoint-independent acl 3000
```

Related commands

nat outbound

display nat eim

nat outbound

Use **nat outbound** to configure an outbound dynamic NAT rule.

Use **undo nat outbound** to delete an outbound dynamic NAT rule.

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

Default

No outbound dynamic NAT rules exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

address-group: Specifies an address group for NAT. If you do not specify an address group, the IP address of the interface is used as the NAT address. Easy IP is used.

group-id: Specifies the address group ID. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the address group name, a case-insensitive string of 1 to 63 characters.

no-pat: Uses the NO-PAT mode. If you do not specify this keyword, PAT is used. PAT only supports TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Enables reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the external network to the internal network.

port-preserved: Tries to preserve port number for PAT. This keyword does not take effect on dynamic NAT port block mapping.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

priority *priority*: Specifies a priority for the rule, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the rule has the lowest priority among the same type of NAT rules.

disable: Disables the outbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

description *text*: Specifies a description for the outbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Outbound dynamic NAT is typically configured on the interface connected to the external network. You can configure multiple outbound dynamic NAT rules on an interface.

Outbound dynamic NAT supports the following modes:

- **PAT**—Performs both IP address translation and port translation. The PAT mode allows external hosts to actively access the internal hosts if the Endpoint-Independent Mapping behavior is used.
- **NO-PAT**—Performs only IP address translation. The NO-PAT mode allows external hosts to actively access the internal hosts if you specify the **reversible** keyword. If an ACL is specified, reverse address translation only applies to packets permitted by ACL reverse matching. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

  Dynamic NAT444 does not support the NO-PAT mode.

When you specify a NAT address group, follow these restrictions and guidelines:

- An address group cannot be used by both the **nat inbound** and **nat outbound** commands.
- An address group cannot be used by the **nat outbound** command in both PAT and NO-PAT modes.
- When port block parameters are specified in the NAT address group, this command configures a dynamic NAT port block mapping. Packets matching the ACL permit rule are processed by dynamic NAT444.

When you specify an ACL, follow these restrictions and guidelines:

- An ACL can be used by only one outbound dynamic NAT rule on an interface.
- If you specify an ACL, NAT translates the source IP addresses of outgoing packets permitted by the ACL into IP addresses in the address group. If you do not specify an ACL, NAT translates all packets.
- Outbound dynamic NAT rules with ACLs configured on an interface takes precedence over those without ACLs. If two ACL-based dynamic NAT rules are configured, the rule with the higher ACL number has higher priority.

Outbound dynamic NAT rules configured with the same priority value and an ACL are matched by using the ACLs in the rule.

- NAT rules with named ACLs have higher priorities than NAT rules with unnamed ACLs.
- NAT rules with named ACLs are matched in alphabetical order of their ACL names.
- NAT rules with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure ACL 2001 to permit packets only from subnet 10.110.10.0/24 to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Create address group 1 and add the address range of 202.110.10.10 to 202.110.10.12 to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an outbound dynamic PAT rule on interface VLAN-interface 10 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1
[Sysname-Vlan-interface10] quit
```

Or

Configure an outbound NO-PAT rule on interface VLAN-interface 10 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1 no-pat
[Sysname-Vlan-interface10] quit
```

Or

Enable Easy IP to use the IP address of VLAN-interface 10 as the translated address.

```
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001
[Sysname-Vlan-interface10] quit
```

Or

Configure an outbound NO-PAT rule on VLAN-interface 10 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1. Enable reverse address translation.

```
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible
```

Related commands

display nat eim

display nat outbound

nat mapping-behavior

nat outbound port-block-group

Use **nat outbound port-block-group** to configure a static outbound port block mapping rule on an interface.

Use **undo nat outbound port-block-group** to delete a static port block mapping rule on an interface.

Syntax

nat outbound port-block-group *group-id* [**rule** *rule-name*] [**counting**]

undo nat outbound port-block-group *group-id*

Default

No static outbound port block mapping rule is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a NAT port block group by its ID. The value range for this argument is 0 to 65535.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

After you configure this command on an interface, the system automatically computes the mappings and creates entries for them. When a private IP address accesses the public network, the private IP address is translated to the mapped public IP address, and the ports are translated to ports in the selected port block.

You can configure multiple port block mapping rules on an interface.

Examples

Configure a static outbound port block mapping rule on VLAN-interface 10, and specify the rule name as **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound port-block-group 1 rule abc
```

Related commands

display nat all

display nat outbound port-block-group

display nat port-block

nat port-block-group

nat outbound rule move

Use **nat outbound rule move** to change the priority of an outbound dynamic NAT rule.

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named outbound dynamic NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the outbound dynamic NAT rule **abc** to the line before the rule **def**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound rule move abc before def
```

Related commands

nat outbound

nat port-block global-share enable

Use **nat port-block global-share enable** to enable port block global sharing.

Use **undo nat port-block global-share enable** to disable port block global sharing.

Syntax

nat port-block global-share enable

undo nat port-block global-share enable

Default

Port block global sharing is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When multiple interfaces have dynamic NAT port block mapping configured, the interfaces might create different port block mappings for packets from the same IP address. You can use this command to configure the interfaces to use the same port block mapping for translating packets from the same IP address.

Examples

Enable port block global sharing.

```
<Sysname> system-view
[Sysname] nat port-block global-share enable
```

Related commands

port-block

nat port-block-group

Use **nat port-block-group** to create a NAT port block group and enter its view, or enter the view of an existing NAT port block group.

Use **undo nat port-block-group** to delete a NAT port block group.

Syntax

nat port-block-group *group-id*

undo nat port-block-group *group-id*

Default

No NAT port block groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Assigns an ID to the NAT port block group. The value range for this argument is 0 to 65535.

Usage guidelines

A NAT port block group is configured to implement static port block mapping for NAT444.

You must configure the following items for a NAT port block group:

- A minimum of one private IP address range (see the **local-ip-address** command).
- A minimum of one public IP address range (see the **global-ip-address** command).
- A port range (see the **port-range** command).
- A port block size (see the **block-size** command).

The system computes static port block mappings according to the port block group configuration, and creates entries for the mappings.

Examples

Create NAT port block group **1**.

```
<Sysname>system-view
[Sysname]nat port-block-group 1
[Sysname-port-block-group-1]
```

Related commands

block-size

display nat all

display nat port-block-group

global-ip-pool

local-ip-address

nat outbound port-block-group

port-range

nat server

Use **nat server** to create a NAT server mapping (also called NAT server rule). The mapping maps the private IP address and port of an internal server to a public address and port.

Use **undo nat server** to delete a NAT server mapping.

Syntax

Common NAT server mapping:

- A single public address with no or a single public port:

nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] **inside** *local-address* [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*]

- A single public address with consecutive public ports:

nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port*1 *local-port*2 } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2*

- Consecutive public addresses with no or a single public port:

nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*]

- Consecutive public addresses with a single public port:

nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* **inside** *local-address local-port*1 *local-port*2 [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** *global-address1 global-address2 global-port*

Load sharing NAT server mapping:

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } **inside server-group** *group-id* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* }

{ *global-port* | *global-port1* *global-port2* } | *global-address1* *global-address2* *global-port* }

ACL-based NAT server mapping:

nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* } **inside** *local-address* [*local-port*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* }

Default

No NAT server mappings exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

protocol *pro-type*: Specifies a protocol type. When the protocol is TCP or UDP, NAT Server can be configured with port information. If you do not specify a protocol type, the command applies to packets of all protocols. The protocol type format can be one of the following:

- A number in the range of 1 to 255.
- A protocol name of **icmp**, **tcp**, or **udp**.

global: Specifies the public network information about the internal server.

global-address: Specifies the public address of an internal server.

global-address1 *global address2*: Specifies a public IP address range, which can include a maximum of 10000 addresses. The *global-address1* argument specifies the start address, and the *global address2* argument specifies the end address that must be greater than the start address.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

current-interface: Enables Easy IP on the current interface. The primary IP address of the interface is used as the public address for the internal server.

interface *interface-type interface-number*: Enables Easy IP on the interface specified by its type and number. The primary IP address of the interface is used as the public address for the internal server. Only loopback interfaces are supported.

global-port1 *global-port2*: Specifies a public port number range, which can include a maximum of 10000 ports. The *global-port1* argument specifies the start port, and the *global-port2* argument specifies the end port that must be greater than the start port. The public port number format can be one of the following:

- A number in the range of 1 to 65535. Both the start port and the end port support this format.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**. Only the start port supports this format.

inside: Specifies the private network information about the internal server.

local-address1 *local-address2*: Specifies a private IP address range. The *local-address1* argument specifies the start address, and the *local-address2* argument specifies the end address that must be greater than the start address. The number of addresses in the range must equal the number of ports in the public port number range.

local-port: Specifies the private port number. The private port number format can be one of the following:

- A number in the range of 1 to 65535, excluding FTP port 20.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**.

global-port: Specifies the public port number. The default value and value range are the same as those for the *local-port* argument.

local-address: Specifies the private IP address.

server-group *group-id*: Specifies the internal server group to which the internal server belongs. With this parameter, the load sharing NAT Server feature is configured. The *group-id* argument specifies the internal server group ID. The value range for the *group-id* argument is 0 to 65535.

acl: Specifies an ACL. If you specify an ACL, only packets permitted by the ACL can be translated by using the mapping.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal servers to the external network. It translates the private IP addresses of the internal servers to their public IP addresses.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the NAT server mapping. If you do not specify this keyword, the mapping is enabled.

description *text*: Specifies a description for the mapping. The *text* argument is a case-insensitive string of 1 to 63 characters.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

You can configure the NAT server mapping to allow servers (such as Web, FTP, Telnet, POP3, and DNS servers) in the internal network to provide services for external users.

NAT server mappings are usually configured on the interface connected to the external network on a NAT device. By using the *global-address* and *global-port* arguments, external users can access the internal server at *local-address* and *local-port*. When the protocol type is not **udp** (protocol number 17) or **tcp** (protocol number 6), you can configure only one-to-one IP address mappings. The following table describes the address-port mappings between an external network and an internal network for NAT Server.

Table 19 Address-port mappings for NAT Server

External network	Internal network
One public address	One private address
One public address and one public port number	One private address and one private port number
One public address and *N* consecutive public port	• One private address and one private port

External network	Internal network
numbers	number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
N consecutive public addresses	• One private address • *N* consecutive private addresses
N consecutive public addresses and one public port number	• One private address and one private port number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
One public address and one public port number	One internal server group
One public address and *N* consecutive public port numbers	
N consecutive public addresses and one public port number	
Public addresses matching an ACL	One private address
	One private address and one private port

The mapping of the protocol type, public address, and public port number must be unique for an internal server on an interface. This restriction also applies when Easy IP is used. The maximum number of NAT server mappings equals the number of public ports in the specified public port range.

As a best practice, do not configure Easy IP for multiple NAT server mappings by using the same interface.

If the IP address of an interface used by Easy IP changes and conflicts with the IP address of a NAT server mapping not using Easy IP, the Easy IP configuration becomes invalid. If the conflicting IP address is modified to another IP address or the NAT server mapping without Easy IP is removed, the Easy IP configuration takes effect.

When you configure a load sharing NAT server mapping, you must make sure a user uses the same public address and public port to access the same service on an internal server. For this purpose, make sure value *N* in the following mappings is equal to or less than the number of servers in the internal server group:

- One public address and *N* consecutive public port numbers are mapped to one internal server group.
- *N* consecutive public addresses and a public port number are mapped to one internal server group.

ACL-based NAT server mappings that are configured with the same priority value are matched by using the ACLs in their rules:

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

An error message for a rollback failure when you perform a configuration rollback for an internal server in the following situation:

- In the running configuration, the name of a NAT server mapping is assigned automatically by the system.
- In the replacement configuration file, the name does not exist.

The system will compare the running configuration file and the replacement file, and display an error message about the mismatch. You can ignore the error message because the NAT server mapping configuration in the configuration file is installed successfully. For example, the NAT server mapping configuration is **nat server global 112.1.1.1 inside 192.168.20.1** in the running configuration, and the is **nat server global 112.1.1.1 inside 192.168.20.1 rule *ServerRule_num*** in the replacement configuration file. After the rollback operation, the new NAT server configuration is successfully installed.

Examples

Allow external users to access the internal Web server at 10.110.10.10 through http://202.110.10.10:8080.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http
[Sysname-Vlan-interface10] quit
```

Configure an ACL-based NAT server mapping to allow users to use IP addresses in subnet 192.168.0.0/24 to access the internal server at 10.0.0.172.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server global 3000 inside 10.0.0.172
```

Related commands

display nat all

display nat server

nat server-group

nat server rule move

Use **nat server rule move** to change the priority of an ACL-based NAT server rule.

Syntax

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named ACL-based NAT server rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the ACL-based NAT server rule **abc** to the line before the ACL-based NAT server rule **def**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server rule move abc before def
```

Related commands

nat server

nat server-group

Use **nat server-group** to create an internal server group and enter its view, or enter the view of an existing internal server group.

Use **undo nat server-group** to delete an internal server group.

Syntax

nat server-group *group-id*

undo nat server-group *group-id*

Default

No internal server groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Assigns an ID to the internal server group.The value range for this argument is 0 to 65535.

Usage guidelines

An internal server group can contain multiple members configured by the **inside ip** command.

Examples

Create internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
```

Related commands

display nat all

display nat server-group

inside ip

nat server

nat static enable

Use **nat static enable** to enable static NAT on an interface.

Use **undo nat static enable** to disable static NAT on an interface.

Syntax

nat static enable

undo nat static enable

Default

Static NAT is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Static NAT mappings take effect on an interface only after static NAT is enabled on the interface.

Examples

Configure an outbound static NAT mapping between private IP address 192.168.1.1 and public IP address 2.2.2.2, and enable static NAT on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat static enable
```

Related commands

display nat all

display nat static

nat static

nat static net-to-net

nat static inbound

Use **nat static inbound** to configure a one-to-one mapping for inbound static NAT.

Use **undo nat static inbound** to delete a one-to-one mapping for inbound static NAT.

Syntax

nat static inbound *global-ip local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound *global-ip local-ip*

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

global-ip: Specifies a public IP address.

local-ip: Specifies a private IP address.

acl: Specifies an ACL to identify the internal hosts that can access the external network.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the internal network to the private IP address.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the one-to-one inbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

When the source IP address of a packet from the external network to the internal network matches the *global-ip*, the source IP address is translated into the *local-ip*. When the destination IP address of a packet from the internal network to the external network matches the *local-ip*, the destination IP address is translated into the *global-ip*.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all incoming packets and the destination address of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the internal network to the private IP address.
- If you specify both an ACL and the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. If packets of connections actively initiated from the internal network to the private IP address are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

One-to-one mappings for inbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an inbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1
```

Related commands

display nat all

display nat static

nat static enable

nat static inbound net-to-net

Use **nat static inbound net-to-net** to configure a net-to-net mapping for inbound static NAT.

Use **undo nat static inbound net-to-net** to remove a net-to-net mapping for inbound static NAT.

Syntax

nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* }

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

global-start-address global-end-address: Specifies a public address range which can contain a maximum of 255 addresses. The *global-end-address* must not be lower than *global-start-address*. If they are the same, only one public address is specified.

local-network: Specifies a private network address.

mask-length: Specifies the mask length of the private network address, in the range of 8 to 31.

mask: Specifies the mask of the private network address.

acl: Specifies an ACL to identify the internal hosts that can access the external network.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the internal network to the private IP addresses.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the net-to-net inbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Specify a public network through a start address and an end address, and a private network through a private address and a mask.

When the source address of a packet from the external network matches the public address range, the source address is translated into a private address in the private address range. When the destination address of a packet from the internal network matches the private address range, the destination address is translated into a public address in the public address range.

The public end address cannot be greater than the greatest IP address in the subnet determined by the public start address and the private network mask. For example, if the private address is 2.2.2.0 with a mask 255.255.255.0 and the public start address is 1.1.1.100, the public end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all incoming packets and the destination address of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the internal network to the private IP addresses.
- If you specify both an ACL and the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. If packets of connections actively initiated from the internal network to the private IP addresses are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

Net-to-net mappings for inbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an inbound static NAT between public network address 202.100.1.0/24 and private network address 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24
```

Related commands

display nat all

display nat static

nat static enable

nat static inbound rule move

Use **nat static inbound rule move** to change the priority of an inbound one-to-one static NAT rule.

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named inbound one-to-one static NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the inbound one-to-one static NAT rule **abc** to the line before the inbound one-to-one static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static inbound rule move abc before def
```

Related commands

nat static inbound

nat static outbound

Use **nat static outbound** to configure a one-to-one mapping for outbound static NAT.

Use **undo nat static outbound** to remove a one-to-one mapping for outbound static NAT.

Syntax

nat static outbound *local-ip global-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound *local-ip global-ip*

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

local-ip: Specifies a private IP address.

global-ip: Specifies a public IP address.

acl: Specifies an ACL to define the destination IP addresses that internal hosts can access.

ipv4-acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the external network to the public IP address.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the one-to-one outbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

When the source IP address of an outgoing packet matches the *local-ip*, the IP address is translated into the *global-ip*. When the destination IP address of an incoming packet matches the *global-ip*, the destination IP address is translated into the *local-ip*.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all outgoing packets and the destination address of all incoming packets are translated.

- If you specify an ACL and do not specify the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the external network to the public IP address.
- If you specify both an ACL and the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. If packets of connections actively initiated from the external network to the public IP address are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

One-to-one mappings for outbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an outbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
```

Configure outbound static NAT, and allow the internal user 192.168.1.1 to access the external network 3.3.3.0/24 by using the public IP address 2.2.2.2.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound 192.168.1.1 2.2.2.2 acl 3001
```

Related commands

display nat all

display nat static

nat static enable

nat static outbound net-to-net

Use **nat static outbound net-to-net** to configure a net-to-net outbound static NAT mapping.

Use **undo nat static outbound net-to-net** to remove the specified net-to-net outbound static NAT mapping.

Syntax

nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name**

ipv4-acl-name } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* }

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

local-start-address local-end-address: Specifies a private address range which can contain a maximum of 255 addresses. The *local-end-address* must not be lower than *local-start-address*. If they are the same, only one private address is specified.

global-network: Specifies a public network address.

mask-length: Specifies the mask length of the public network address, in the range of 8 to 31.

mask: Specifies the mask of the public network address.

acl: Specifies an ACL to define the destination IP addresses that internal hosts can access.

ipv4-acl-number: Specifies an ACL number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the external network to the public IP addresses.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the net-to-net outbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Specify a private network through a start address and an end address, and a public network through a public address and a mask.

When the source address of a packet from the internal network matches the private address range, the source address is translated into a public address in the public address range. When the destination address of a packet from the external network matches the public address range, the destination address is translated into a private address in the private address range.

The private end address cannot be greater than the greatest IP address in the subnet determined by the private start address and the public network mask. For example, the public address is 2.2.2.0 with a mask 255.255.255.0, and the private start address is 1.1.1.100. The private end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all outgoing packets and the destination address of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the external network to the public IP addresses.
- If you specify both an ACL and the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. If packets of connections actively initiated from the external network to the public IP addresses are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

Net-to-net mappings for outbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an outbound static NAT mapping between private network address 192.168.1.0/24 and public network address 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24
```

Configure outbound static NAT. Allow internal users on subnet 192.168.1.0/24 to access the external subnet 3.3.3.0/24 by using public IP addresses on subnet 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl
3001
```

Related commands

display nat all

display nat static

nat static enable

nat static outbound rule move

Use **nat static outbound rule move** to change the priority of an outbound one-to-one static NAT rule.

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named outbound one-to-one static NAT rules..

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the outbound one-to-one static NAT rule **abc** to the line before the outbound one-to-one static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static outbound rule move abc before def
```

Related commands

nat static outbound

nat timestamp delete

Use **nat timestamp delete** to enable the deletion of timestamps in TCP SYN and SYN ACK packets.

Use **undo nat timestamp delete** to restore the default.

Syntax

nat timestamp delete

undo nat timestamp delete

Default

The TCP SYN and SYN ACK packets carry the timestamp.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If PAT mode is configured on an interface by using **nat inbound** or **nat outbound**, and the tcp_timestamp and tcp_tw_recycle function is configured on the TCP server, TCP connections might not be established. To solve the problem, you can shut down the tcp_tw_recycle function or configure the **nat timestamp delete** command.

Examples

Enable the deletion of the timestamp for TCP SYN and SYN ACK packets on the public network.

```
<Sysname> system-view
[Sysname] nat timestamp delete
```

Related commands

nat outbound

nat inbound

port-block

Use **port block** to configure port block parameters for a NAT address group.

Use **undo port block** to restore the default.

Syntax

port block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port block

Default

No port block parameters are configured for a NAT address group.

Views

NAT address group view

Predefined user roles

network-admin

Parameters

block-size *block-size*: Specifies the port block size. The value range for the *block-size* argument is 1 to 65535. In a NAT address group, the port block size cannot be larger than the number of ports in the port range.

extended-block-number *extended-block-number*: Specifies the number of extended port blocks, in the range of 1 to 5. When a private IP address accesses the public network, but the ports in the selected port block are all occupied, the NAT444 gateway extends port blocks one by one for the private IP address.

Usage guidelines

To configure dynamic port block mappings, port block parameters are required in the NAT address group. When a private IP address initiates a connection to the public network, the NAT444 gateway assigns it a public IP address and a port block, and creates an entry for the mapping. For subsequent connections from the private IP address, the NAT444 gateway translates the private IP address to the mapped public IP address and the ports to ports in the selected port block.

Examples

Set the port block size to 256 and the number of extended port blocks to 1 in NAT address group 2.

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

```
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1
```

Related commands

nat address-group

port-range

Use **port-range** to specify a port range for public IP addresses.

Use **undo port-range** to restore the default.

Syntax

port-range *start-port-number end-port-number*

undo port-range

Default

The port range for public IP addresses is 1 to 65535.

Views

NAT address group view

NAT port block group view

Predefined user roles

network-admin

Parameters

start-port-number end-port-number: Specifies the start port number and end port number for the port range. The end port number cannot be smaller than the start port number. As a best practice, set the start port number to be equal to or larger than 1024 to avoid an application protocol identification error.

Usage guidelines

The port range must include all ports that public IP addresses use for address translation.

The number of ports in a port range cannot be smaller than the port block size.

Examples

Specify the port range as 1024 to 65535 for NAT address group 1.

```
<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-range 1024 65535
```

Specify the port range as 30001 to 65535 for NAT port block group 1.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-range 30001 65535
```

Related commands

nat address-group

nat port-block-group

reset nat count statistics

Use **reset nat count statistics** to clear NAT counting statistics.

Syntax

reset nat count statistics { **all** | **dynamic** | **server** | **static** | **static-port-block** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all counting statistics for NAT mappings.

dynamic: Clears counting statistics for dynamic NAT mappings.

server: Clears counting statistics for NAT server mappings.

static: Clears counting statistics for static NAT mappings.

static-port-block: Clears counting statistics for NAT444 mappings.

Examples

Clear all counting statistics for static NAT mappings.

```
<Sysname> reset nat count statistics all
```

Related commands

display nat inbound

display nat outbound

display nat outbound port-block-group

display nat port-block

display nat static

display nat server

reset nat session

Use **reset nat session** to clear NAT sessions.

Syntax

In standalone mode:

reset nat session

In IRF mode:

reset nat session [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears NAT sessions for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Clear all NAT sessions.

```
<Sysname> reset nat session
```

(In IRF mode.) Clear NAT sessions for the specified slot.

```
<Sysname> reset nat session slot 1
```

Related commands

display nat session

Contents

IP performance optimization commands ····· 1

display icmp statistics ····· 1
display ip statistics ····· 2
display rawip ····· 3
display rawip verbose ····· 4
display tcp ····· 8
display tcp statistics ····· 9
display tcp verbose ····· 11
display tcp-proxy ····· 16
display tcp-proxy port-info ····· 18
display udp ····· 21
display udp statistics ····· 21
display udp verbose ····· 22
ip forward-broadcast ····· 26
ip icmp error-interval ····· 27
ip icmp source ····· 28
ip mtu ····· 28
ip reassemble local enable ····· 29
ip redirects enable ····· 30
ip ttl-expires enable ····· 30
ip unreachables enable ····· 31
reset ip statistics ····· 32
reset tcp statistics ····· 33
reset udp statistics ····· 33
tcp mss ····· 33
tcp path-mtu-discovery ····· 34
tcp syn-cookie enable ····· 35
tcp timer fin-timeout ····· 36
tcp timer syn-timeout ····· 36
tcp window ····· 37

IP performance optimization commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

display icmp statistics

Use **display icmp statistics** to display ICMP statistics.

Syntax

In standalone mode:

display icmp statistics

In IRF mode:

display icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMP statistics for all member devices. (In IRF mode.)

Usage guidelines

ICMP statistics include information about received and sent ICMP packets.

Examples

Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                   bad checksum            0
         echo          175                 destination unreachable 0
         source quench 0                   redirects               0
         echo replies  201                 parameter problem       0
         timestamp     0                   information requests    0
         mask requests 0                   mask replies            0
         time exceeded 0                   invalid type            0
         router advert 0                   router solicit          0
         broadcast/multicast echo requests ignored           0
         broadcast/multicast timestamp requests ignored      0
 Output: echo          0                   destination unreachable 0
         source quench 0                   redirects               0
         echo replies  175                 parameter problem       0
         timestamp     0                   information replies     0
         mask requests 0                   mask replies            0
         time exceeded 0                   bad address             0
         packet error  1442                router advert           3
```

display ip statistics

Use **display ip statistics** to display IP packet statistics.

Syntax

In standalone mode:

display ip statistics

In IRF mode:

display ip statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IP packet statistics for all member devices. (In IRF mode.)

Usage guidelines

IP statistics include information about received and sent packets, fragments, and reassembly.

Examples

Display IP packet statistics.

```
<Sysname> display ip statistics
  Input:           sum            7120          local             112
                   bad protocol   0             bad format        0
                   bad checksum   0             bad options       0
                   dropped        0
  Output:          forwarding     0             local             27
                   dropped        0             no route          2
                   compress fails 0
  Reassembling:    fragments      0             reassembled       0
                   dropped        0             timeouts          0
  Fragment:        fragmented     0             couldn't fragment 0
                   output frags   0
  Forwarded Frags: sum            0
```

Table 1 Command output

Field	Description
Input	Statistics about received packets: • **sum**—Total number of packets received. • **local**—Total number of packets destined for the device. • **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. • **dropped**—Total number of incoming packets that have been dropped.

Field	Description
Output	Statistics about outgoing packets: • **forwarding**—Total number of forwarded packets. • **local**—Total number of packets sent from the local device. • **dropped**—Total number of outgoing packets that have been dropped. • **no route**—Total number of packets with no routes available. • **compress fails**—Total number of packets with compression failures.
Reassembling	Statistics about reassembling: • **fragments**—Total number of fragments that need reassembling. • **reassembled**—Total number of packets that are reassembled. • **dropped**—Total number of dropped fragments that fail the reassembling. • **timeouts**—Total number of reassembly timeouts.
Fragment	Statistics about fragments: • **fragmented**—Total number of packets successfully fragmented. • **couldn't fragment**—Total number of packets that failed to be fragmented. • **output**—Total number of fragments sent.
Forwarded Frags	Statistics about forwarded fragments: • **sum**—Total number of fragments that are directly forwarded.

Related commands

`display ip interface`

`reset ip statistics`

display rawip

Use **`display rawip`** to display brief information about RawIP connections.

Syntax

In standalone mode:

`display rawip`

In IRF mode:

`display rawip` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about RawIP connections for all member devices. (In IRF mode.)

Usage guidelines

Brief RawIP connection information includes local and peer addresses, protocol, and PCB.

Examples

(In standalone mode.) Display brief information about RawIP connections.

```
<Sysname> display rawip
 Local Addr       Foreign Addr     Protocol  PCB
 0.0.0.0          0.0.0.0          1         0x0000000000000009
 0.0.0.0          0.0.0.0          1         0x0000000000000008
 0.0.0.0          0.0.0.0          1         0x0000000000000002
```

(In IRF mode.) Display brief information about RawIP connections.

```
<Sysname> display rawip
 Local Addr       Foreign Addr     Protocol  Slot  CPU PCB
 0.0.0.0          0.0.0.0          1         1     0   0x0000000000000009
 0.0.0.0          0.0.0.0          1         1     0   0x0000000000000008
 0.0.0.0          0.0.0.0          1         5     0   0x0000000000000002
```

Table 2 Command output

Field	Description
Local Addr	Local IP address.
Foreign Addr	Peer IP address.
Protocol	Protocol number.
PCB	Protocol control block.

display rawip verbose

Use **display rawip verbose** to display detailed information about RawIP connections.

Syntax

In standalone mode:

display rawip verbose [**pcb** *pcb-index*]

In IRF mode:

display rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed RawIP connection information for the specified PCB. The *pcb-index* argument specifies the index of the PCB. The index value range is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about RawIP connections for all member devices. (In IRF mode.)

Usage guidelines

The detailed information includes socket creator, state, option, type, protocol number, and the source and destination IP addresses of RawIP connections.

Examples

(In standalone mode.) Display detailed information about RawIP connections.

```
<Sysname> display rawip verbose
Total RawIP socket number: 1

 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

(In IRF mode.) Display detailed information about RawIP connections.

```
<Sysname> display rawip verbose
Total RawIP socket number: 1

 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Location: slot: 6
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 3 Command output

Field	Description
Total RawIP socket number	Total number of RawIP sockets.

Field	Description
Connection info	Connection information, including source IP address and destination IP address.
Location	Socket location.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_FILTER**—Supports setting the packet filter criterion. This option takes effect on incoming packets. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **N/A**—No options are set.
Error	Error code.
Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.

Field	Description
Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SNDBYLSPV**—Sends through MPLS. This field is not supported in the current software version. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_USEICMPSRC**—Uses the specified IP address as the source IP address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet.

Field	Description
	• **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display tcp

Use **display tcp** to display brief information about TCP connections.

Syntax

In standalone mode:

display tcp

In IRF mode:

display tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about TCP connections for all member devices. (In IRF mode.)

Usage guidelines

Brief TCP connection information includes local IP address, local port number, peer IP address, peer port number, and TCP connection state.

Examples

(In standalone mode.) Display brief information about TCP connections.

```
<Sysname> display tcp
 *: TCP MD5 Connection
 Local Addr:port       Foreign Addr:port     State       PCB
*0.0.0.0:21            0.0.0.0:0             LISTEN      0x000000000000c387
```

```
 192.168.20.200:23     192.168.20.14:1284    ESTABLISHED 0x0000000000000009
 192.168.20.200:23     192.168.20.14:1283    ESTABLISHED 0x0000000000000002
```

(In IRF mode.) Display brief information about TCP connections.

```
<Sysname> display tcp
 *: TCP MD5 Connection
 Local Addr:port       Foreign Addr:port     State       Slot  CPU PCB
*0.0.0.0:21            0.0.0.0:0             LISTEN      1     0   0x000000000000c387
 192.168.20.200:23     192.168.20.14:1284    ESTABLISHED 1     0   0x0000000000000009
 192.168.20.200:23     192.168.20.14:1283    ESTABLISHED 1     0   0x0000000000000002
```

Table 4 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
PCB	PCB index.

display tcp statistics

Use **display tcp statistics** to display TCP traffic statistics.

Syntax

In standalone mode:

display tcp statistics

In IRF mode:

display tcp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays TCP traffic statistics for all member devices. (In IRF mode.)

Usage guidelines

TCP traffic statistics include information about received and sent TCP packets and Syncache/syncookie.

Examples

Display TCP traffic statistics.

```
<Sysname> display tcp statistics
Received packets:
    Total: 4150
```

```
        packets in sequence: 1366 (134675 bytes)
        window probe packets: 0, window update packets: 0
        checksum error: 0, offset error: 0, short error: 0
        packets dropped for lack of memory: 0
        packets dropped due to PAWS: 0
        duplicate packets: 12 (36 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: 3531 (795048 bytes)
        duplicate ACK packets: 33, ACK packets for unsent data: 0

    Sent packets:
        Total: 4058
        urgent packets: 0
        control packets: 50
        window probe packets: 3, window update packets: 11
        data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
        ACK-only packets: 150 (52 delayed)
        unnecessary packet retransmissions: 0

    Syncache/syncookie related statistics:
        entries added to syncache: 12
        syncache entries retransmitted: 0
        duplicate SYN packets: 0
        reply failures: 0
        successfully build new socket: 12
        bucket overflows: 0
        zone failures: 0
        syncache entries removed due to RST: 0
        syncache entries removed due to timed out: 0
        ACK checked by syncache or syncookie failures: 0
        syncache entries aborted: 0
        syncache entries removed due to bad ACK: 0
        syncache entries removed due to ICMP unreachable: 0
        SYN cookies sent: 0
        SYN cookies received: 0

    SACK related statistics:
        SACK recoveries: 1
        SACK retransmitted segments: 0 (0 bytes)
        SACK blocks (options) received: 0
        SACK blocks (options) sent: 0
        SACK scoreboard overflows: 0

    Other statistics:
        retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
        persist timeout: 0
```

```
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped due to MD5 authentication failure: 0
    packets that passed MD5 authentication: 0
    sent Keychain-encrypted packets: 0
    packets that passed Keychain authentication: 0
    packets dropped due to Keychain authentication failure: 0
    packets dropped with MD5 authentication: 0
    packets permitted with MD5 authentication: 0
```

Related commands

reset tcp statistics

display tcp verbose

Use **display tcp verbose** to display detailed information about TCP connections.

Syntax

In standalone mode:

display tcp verbose [**pcb** *pcb-index*]

In IRF mode:

display tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed TCP connection information for the specified PCB. The index value range is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about TCP connections for all member devices. (In IRF mode.)

Usage guidelines

The detailed TCP connection information includes socket creator, state, option, type, protocol number, source IP address and port number, destination IP address and port number, and connection state.

Examples

(In standalone mode.) Display detailed information about TCP connections.

```
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

(In IRF mode.) Display detailed information about TCP connections.

```
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Location: slot: 6
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat /state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
```

```
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

Table 5 Command output

Field	Description
TCP inpcb number	Number of TCP IP PCBs.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location.
NSR standby	This field is not supported in the current software version. ID of the IRF member device and number of the slot where the NSR standby card resides. This field displays **N/A** if no NSR standby card is present.
tcpcb number	Number of TCP PCBs. This field is not displayed if the state of the TCP connection is **TIME_WAIT**.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	State of the socket: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. • **N/A**—No options are set.

Field	Description
Error	Error code.
Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SNDBYLSPV**—Sends through MPLS. This value is not supported in the current software version.

Field	Description
	• **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_PASSWORD**—Password is set. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option.
NSR state	NSR state of the TCP connection: • **CLOSED**—Closed (initial) state. • **CLOSING**—The connection is to be closed. • **ENABLED**—The connection backup is enabled. • **OPEN**—The connection synchronization has started. • **PENDING**—The connection backup is not ready. • **READY**—The connection backup is ready. • **SMOOTH**—The connection data is being smoothed. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display tcp-proxy

Use **display tcp-proxy** to display brief information about TCP proxy.

Syntax

In standalone mode:

display tcp-proxy

In IRF mode:

display tcp-proxy slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: • WX2540H • WX2540H-F • WX2560H No: • WX2508H-PWR-LTE • WX2510H-PWR • WX2510H-F-PWR
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-X-PWR • WX3010H-L-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes: WX5510E No: WX5540E
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No

Hardware series	Model	Product code	Command compatibility
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Usage guidelines

TCP proxy splits every TCP connection that passes through it into two TCP connections to relay data packets between clients and servers. The split is transparent to the servers and clients. This feature reduces bandwidth use and improves TCP performance. It is used for services such as load balancing.

Examples

(In standalone mode.) Display brief information about TCP proxy.

```
<Sysname> display tcp-proxy
Local Addr:port       Foreign Addr:port     State        Service type
192.168.56.25:1111    111.111.111.125:8080  ESTABLISHED  LB
111.111.111.125:8080  192.168.56.25:1111    ESTABLISHED  LB
```

(In IRF mode.) Display brief information about TCP proxy for the specified slot.

```
<Sysname> display tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State        Service type
192.168.56.25:1111    111.111.111.125:8080  ESTABLISHED  LB
111.111.111.125:8080  192.168.56.25:1111    ESTABLISHED  LB
```

Table 6 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
Service type	Type of services that the TCP proxy is used for: • **LB**—Load balancing services.

display tcp-proxy port-info

Use **display tcp-proxy port-info** to display the usage of non-well known ports for TCP proxy.

Syntax

In standalone mode:

display tcp-proxy port-info

In IRF mode:

display tcp-proxy port-info slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: • WX2540H • WX2540H-F • WX2560H • No: • WX2508H-PWR-LTE • WX2510H • WX2510H-F
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L • WX3010H-X • WX3024H-L
WX3500H series	WX3508H WX3508H WX3510H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H	Yes

Hardware series	Model	Product code	Command compatibility
	WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes: WX5510E No: WX5540E
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays non-well known port usage for all member devices. (In IRF mode.)

Usage guidelines

The TCP ports are divided into well-known ports (port numbers from 0 through 1023) and non-well known ports (port numbers from 1024 through 65535).

- Well known ports are for certain services, for example, port 23 for Telnet service, ports 20 and 21 for FTP service, and port 80 for HTTP service.
- Non-well known ports are available for various services. You can use the **display tcp-proxy port-info** command to display the usage of these ports.

Examples

(In standalone mode.) Display the usage of non-well known ports for TCP proxy.

```
<Sysname> display tcp-proxy port-info
Index  Range            State
16     [1024, 1087]     USABLE
17     [1088, 1151]     USABLE
18     [1152, 1215]     USABLE
19     [1216, 1279]     USABLE
20     [1280, 1343]     USABLE
...
1020   [65280, 65343]   USABLE
1021   [65344, 65407]   USABLE
1022   [65408, 65471]   USABLE
1023   [65472, 65535]   USABLE
```

(In IRF mode.) Display the usage of non-well known ports for TCP proxy for the specified slot.

```
<Sysname> display tcp-proxy port-info slot 1
Index  Range            State
16     [1024, 1087]     USABLE
17     [1088, 1151]     USABLE
18     [1152, 1215]     USABLE
19     [1216, 1279]     USABLE
20     [1280, 1343]     USABLE
...
1020   [65280, 65343]   USABLE
1021   [65344, 65407]   USABLE
1022   [65408, 65471]   USABLE
1023   [65472, 65535]   USABLE
```

Table 7 Command output

Field	Description
Index	Index of the port range.
Range	Start port number and end port number.
State	State of the port range: • **USABLE**—The ports are assignable. • **ASSIGNED**—Some ports are dynamically assigned and some ports are not. • **ALLASSIGNED**—All ports are dynamically assigned. The assigned ports can be reclaimed. • **TO RECLAIM**—Some ports are statically assigned. The assigned ports can be reclaimed. • **RESERVED**—The ports are reserved. The reserved ports cannot be dynamically assigned.

display udp

Use **display udp** to display brief information about UDP connections.

Syntax

In standalone mode:

display udp

In IRF mode:

display udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about UDP connections for all member devices. (In IRF mode.)

Usage guidelines

Brief UDP connection information includes local IP address and port number, and peer IP address and port number.

Examples

(In standalone mode.) Display brief information about UDP connections.

```
<Sysname> display udp
 Local Addr:port        Foreign Addr:port      PCB
 0.0.0.0:69             0.0.0.0:0              0x0000000000000003
 192.168.20.200:1024    192.168.20.14:69       0x0000000000000002
```

(In IRF mode.) Display brief information about UDP connections.

```
<Sysname> display udp
 Local Addr:port        Foreign Addr:port     Slot  CPU PCB
 0.0.0.0:69             0.0.0.0:0             1     0   0x0000000000000003
 192.168.20.200:1024    192.168.20.14:69      5     0   0x0000000000000002
```

Table 8 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
PCB	PCB index.

display udp statistics

Use **display udp statistics** to display UDP traffic statistics.

Syntax

In standalone mode:

display udp statistics

In IRF mode:

display udp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays UDP traffic statistics for all member devices. (In IRF mode.)

Usage guidelines

UDP traffic statistics include information about received and sent UDP packets.

Examples

Display UDP traffic statistics.

```
<Sysname> display udp statistics
Received packets:
     Total: 240
     checksum error: 0, no checksum: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port(unicast): 0
     no socket on port(broadcast/multicast): 240
     not delivered, input socket full: 0
Sent packets:
     Total: 0
```

Related commands

reset udp statistics

display udp verbose

Use **display udp verbose** to display detailed information about UDP connections.

Syntax

In standalone mode:

display udp verbose [**pcb** *pcb-index*]

In IRF mode:

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed UDP connection information for the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about UDP connections for all member devices. (In IRF mode.)

Usage guidelines

The detailed information includes socket creator, status, option, type, protocol number, source IP address and port number, and destination IP address and port number for UDP connections.

Examples

(In standalone mode.) Display detailed UDP connection information.

```
<Sysname> display udp verbose
Total UDP socket number: 1

 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

(In IRF mode.) Display detailed UDP connection information.

```
<Sysname> display udp verbose
Total UDP socket number: 1

 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Location: Slot: 6
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
```

```
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

Table 9 Command output

Field	Description
Total UDP socket number	Total number of UDP sockets.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-o-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space.

Field	Description
	• **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SNDBYLSPV**—Sends through MPLS. This value is not supported in the current software version. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.

Field	Description
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

ip forward-broadcast

Use **ip forward-broadcast** to enable an interface to receive and forward directed broadcast packets destined for the directly connected network.

Use **undo ip forward-broadcast** to disable an interface from receiving and forwarding directed broadcast packets destined for the directly connected network.

Syntax

ip forward-broadcast

undo ip forward-broadcast

Default

An interface cannot forward directed broadcasts destined for the directly connected network, and can receive directed broadcasts destined for the directly connected network.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl *acl-number*: Specifies an ACL by its number. The interface forwards only the directed broadcasts permitted by the ACL. The value range for basic ACLs is 2000 to 2999. The value range for advanced ACLs is 3000 to 3999.

Usage guidelines

A directed broadcast packet is destined for all hosts on a specific network. In the destination IP address of the directed broadcast, the network ID identifies the target network, and the host ID is made up of all ones.

This command enables an interface to accept and forward the following directed broadcast packets:

- Accept directed broadcast packets that are destined for and received from the directly connected network.
- Forward directed broadcast packets that are destined for the directly connected network and are received from another subnet.

Hackers can use directed broadcast packets to attack the target network. In some scenarios, however, an interface must receive and send directed broadcast packets to support Wake on LAN. Wake on LAN sends the directed broadcasts to wake up the hosts on the target network.

In this case, you can execute this command to enable the interface to receive and forward directed broadcast packets destined for the directly connected network.

Examples

Enable VLAN-interface 2 to receive and forward directed broadcast packets destined for the directly connected network.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast
```

ip icmp error-interval

Use **ip icmp error-interval** to set the interval for tokens to arrive in the bucket for ICMP error messages and the bucket size.

Use **undo ip icmp error-interval** to restore the default.

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

Default

A token is placed in the bucket every 100 milliseconds, and the bucket allows a maximum of 10 tokens.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMP rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMP error messages are sent. Use this command to avoid sending excessive ICMP error messages within a short period that might cause network congestion. A token bucket algorithm is used with one token representing one ICMP error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMP error message is sent. When the bucket is empty, ICMP error messages are not sent until a new token is placed in the bucket.

Examples

Set the interval to 200 milliseconds for tokens to arrive in the bucket for ICMP error messages, and set the bucket size to 40 tokens.

```
<Sysname> system-view
[Sysname] ip icmp error-interval 200 40
```

ip icmp source

Use **ip icmp source** to specify the source address for outgoing ICMP packets.

Use **undo ip icmp source** to remove the specified source address for outgoing ICMP packets.

Syntax

ip icmp source *ip-address*

undo ip icmp source

Default

No source address is specified for outgoing ICMP packets. The default source IP addresses for different types of ICMP packets vary as follows:

- For an ICMP error message, the source IP address is the IP address of the receiving interface of the packet that triggers the ICMP error message. ICMP error messages include Time Exceeded, Port Unreachable, and Parameter Problem messages.
- For an ICMP echo request, the source IP address is the IP address of the sending interface.
- For an ICMP echo reply, the source IP address is the destination IP address of the ICMP echo request specific to this reply.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address.

Usage guidelines

It is a good practice to specify the IP address of the loopback interface as the source IP address for outgoing ping echo request and ICMP error messages. This feature helps users to locate the sending device easily.

Examples

Specify 1.1.1.1 as the source address for outgoing ICMP packets.

```
<Sysname> system-view
[Sysname] ip icmp source 1.1.1.1
```

ip mtu

Use **ip mtu** to set the interface MTU for IPv4 packets. The MTU defines the largest size of an IPv4 packet that an interface can transmit without fragmentation.

Use **undo ip mtu** to restore the default.

Syntax

ip mtu *mtu-size*

undo ip mtu

Default

The interface MTU is not set.

Views

Interface view

Predefined user roles

network-admin

Parameters

mtu-size: Specifies the MTU in bytes. The value range for the *mtu-size* argument varies by interface type.

Usage guidelines

When a packet exceeds the MTU of the sending interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Fragmentation and reassembling consume system resources, so set an appropriate MTU to avoid fragmentation.

If an interface supports both the **mtu** and **ip mtu** commands, the device fragments a packet based on the MTU set by the **ip mtu** command.

Examples

Set the MTU to 1280 bytes for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip mtu 1280
```

ip reassemble local enable

Use **ip reassemble local enable** to enable IPv4 local fragment reassembly.

Use **undo ip reassemble local enable** to disable local fragment reassembly.

Syntax

ip reassemble local enable

undo ip reassemble local enable

Default

IPv4 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature on a multichassis IRF fabric to improve fragment reassembly efficiency. This feature enables a subordinate to reassemble the IPv4 fragments of a packet if all the fragments arrive at it. If this feature is disabled, all IPv4 fragments are delivered to the master device for reassembly. The feature applies only to fragments destined for the same subordinate.

Examples

Enable IPv4 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ip reassemble local enable
```

ip redirects enable

Use **ip redirects enable** to enable sending ICMP redirect messages.

Use **undo ip redirects enable** to disable sending ICMP redirect messages.

Syntax

ip redirects enable

undo ip redirects enable

Default

Sending ICMP redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMP redirect messages simplify host management and enable hosts to gradually optimize their routing tables.

A host that has only one route destined for the default gateway sends all packets to the default gateway. The default gateway sends an ICMP redirect message to inform the host of a correct next hop when the following conditions are met:

- The receiving and sending interfaces are the same.
- The packet source IP address and the IP address of the packet receiving interface are on the same segment.
- There is no source route option in the received packet.

Examples

Enable sending ICMP redirect messages.

```
<Sysname> system-view
[Sysname] ip redirects enable
```

ip ttl-expires enable

Use **ip ttl-expires enable** to enable sending ICMP time exceeded messages.

Use **undo ip ttl-expires enable** to disable sending ICMP time exceeded messages.

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

Default

Sending ICMP time exceeded messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP time exceeded messages by following these rules:

- The device sends an ICMP TTL exceeded in transit message to the source when the following conditions are met:
  - The received packet is not destined for the device.
  - The TTL field of the packet is 1.
- When the device receives the first fragment of an IP datagram destined for the device itself, it starts a timer. If the timer expires before all the fragments of the datagram are received, the device sends an ICMP fragment reassembly time exceeded message to the source.

A device disabled from sending ICMP time exceeded messages does not send ICMP TTL exceeded in transit messages but can still send ICMP fragment reassembly time exceeded messages.

Examples

Enable sending ICMP time exceeded messages.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachables enable

Use **ip unreachables enable** to enable sending ICMP destination unreachable messages.

Use **undo ip unreachables enable** to disable sending ICMP destination unreachable messages.

Syntax

ip unreachables enable

undo ip unreachables enable

Default

Sending ICMP destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP destination unreachable messages by following these rules:

- The device sends the source an ICMP network unreachable message when the following conditions are met:
  - The received packet does not match any route.
  - No default route exists in the routing table.
- The device sends the source an ICMP protocol unreachable message when the following conditions are met:
  - The received packet is destined for the device.
  - The transport layer protocol of the packet is not supported by the device.
- The device sends the source an ICMP port unreachable message when the following conditions are met:
  - The received UDP packet is destined for the device.
  - The packet's port number does not match the running process.
- The device sends the source an ICMP source route failed message when the following conditions are met:
  - The source uses Strict Source Routing to send packets.
  - The intermediate device finds that the next hop specified by the source is not directly connected.
- The device sends the source an ICMP fragmentation needed and DF set message when the following conditions are met:
  - The MTU of the sending interface is smaller than the packet.
  - The packet has Don't Fragment set.

Examples

Enable sending ICMP destination unreachable messages.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

reset ip statistics

Use **reset ip statistics** to clear IP traffic statistics.

Syntax

In standalone mode:

reset ip statistics

In IRF mode:

reset ip statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IP traffic statistics for all member devices. (In IRF mode.)

Usage guidelines

Use this command to clear history IP traffic statistics before you collect IP traffic statistics for a time period.

Examples

Clear IP traffic statistics.

```
<Sysname> reset ip statistics
```

Related commands

display ip interface

display ip statistics

reset tcp statistics

Use **reset tcp statistics** to clear TCP traffic statistics.

Syntax

reset tcp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear TCP traffic statistics.

```
<Sysname> reset tcp statistics
```

Related commands

display tcp statistics

reset udp statistics

Use **reset udp statistics** to clear UDP traffic statistics.

Syntax

reset udp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear UDP traffic statistics.

```
<Sysname> reset udp statistics
```

Related commands

display udp statistics

tcp mss

Use **tcp mss** to set the TCP maximum segment size (MSS).

Use **undo tcp mss** to restore the default.

Syntax

tcp mss *value*

undo tcp mss

Default

The TCP MSS is not set.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the TCP MSS in bytes. The minimum value is 128 bytes. The maximum value equals the maximum MTU that the interface supports minus 40.

Usage guidelines

The MSS option informs the receiver of the largest segment that the sender can accept. Each end announces its MSS during TCP connection establishment. If the size of a TCP segment is smaller than the MSS of the receiver, TCP sends the TCP segment without fragmentation. If not, TCP fragments the segment according to the receiver's MSS.

If you set the TCP MSS on an interface, the size of each TCP segment received or sent on the interface cannot exceed the MSS value.

This configuration takes effect only on TCP connections that are established after the configuration and not on the TCP connections that already exist.

This configuration is effective only on IP packets.

Examples

Set the TCP MSS to 300 bytes on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] tcp mss 300
```

tcp path-mtu-discovery

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery.

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

Default

TCP path MTU discovery is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging *age-time*: Specifies the aging time for the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Does not age out the path MTU.

Usage guidelines

After you enable TCP path MTU discovery, all new TCP connections detect the path MTU. The device uses the path MTU to calculate the MSS to avoid IP fragmentation.

After you disable TCP path MTU discovery, the system stops all path MTU timers. The TCP connections established later do not detect the path MTU, but the TCP connections previously established still can detect the path MTU.

Examples

Enable TCP path MTU discovery and set the path MTU aging time to 20 minutes.

```
<Sysname> system-view
[Sysname] tcp path-mtu-discovery aging 20
```

tcp syn-cookie enable

Use **tcp syn-cookie enable** to enable SYN Cookie to protect the device from SYN flood attacks.

Use **undo tcp syn-cookie enable** to disable SYN Cookie.

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

Default

SYN Cookie is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A TCP connection is established through a three-way handshake:

1. The sender sends a SYN packet to the server.
2. The server receives the SYN packet, establishes a TCP semi-connection in SYN_RECEIVED state, and replies with a SYN ACK packet to the sender.
3. The sender receives the SYN ACK packet and replies with an ACK packet. Then, a TCP connection is established.

An attacker can exploit this mechanism to mount SYN flood attacks. The attacker sends a large number of SYN packets, but they do not respond to the SYN ACK packets from the server. As a result, the server establishes a large number of TCP semi-connections and cannot handle normal services.

SYN Cookie can protect the server from SYN flood attacks. When the server receives a SYN packet, it responds to the request with a SYN ACK packet without establishing a TCP semi-connection.

The server establishes a TCP connection and enters ESTABLISHED state only when it receives an ACK packet from the sender.

Examples

Enable SYN Cookie.

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

tcp timer fin-timeout

Use **tcp timer fin-timeout** to set the TCP FIN wait timer.

Use **undo tcp timer fin-timeout** to restore the default.

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

Default

The TCP FIN wait timer is 675 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP FIN wait timer in the range of 76 to 3600 seconds.

Usage guidelines

TCP starts the FIN wait timer when the state of a TCP connection changes to FIN_WAIT_2. If no FIN packet is received within the timer interval, the TCP connection is terminated.

If a FIN packet is received, TCP changes the connection state to TIME_WAIT. If a non-FIN packet is received, TCP restarts the timer and tears down the connection when the timer expires.

Examples

Set the TCP FIN wait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Use **tcp timer syn-timeout** to set the TCP SYN wait timer.

Use **undo tcp timer syn-timeout** to restore the default.

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

Default

The TCP SYN wait timer is 75 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP SYN wait timer in the range of 2 to 600 seconds.

Usage guidelines

TCP starts the SYN wait timer after sending a SYN packet. Within the SYN wait timer if no response is received or the upper limit on TCP connection tries is reached, TCP fails to establish the connection.

Examples

Set the TCP SYN wait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Use **tcp window** to set the size of the TCP receive/send buffer.

Use **undo tcp window** to restore the default.

Syntax

tcp window *window-size*

undo tcp window

Default

The size of the TCP receive/send buffer is 63 KB.

Views

System view

Predefined user roles

network-admin

Parameters

window-size: Specifies the size of the TCP receive/send buffer, in the range of 1 to 64 KB.

Examples

Set the size of the TCP receive/send buffer to 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

Contents

IPv6 basics commands 1

display ipv6 fib 1
display ipv6 icmp statistics 2
display ipv6 interface 4
display ipv6 interface prefix 8
display ipv6 nd snooping 9
display ipv6 nd snooping count 10
display ipv6 neighbors 11
display ipv6 neighbors count 13
display ipv6 pathmtu 13
display ipv6 prefix 14
display ipv6 rawip 16
display ipv6 rawip verbose 17
display ipv6 statistics 20
display ipv6 tcp 24
display ipv6 tcp verbose 25
display ipv6 tcp-proxy 30
display ipv6 tcp-proxy port-info 33
display ipv6 udp 35
display ipv6 udp verbose 36
ipv6 address 40
ipv6 address anycast 41
ipv6 address auto 41
ipv6 address auto link-local 42
ipv6 address eui-64 43
ipv6 address link-local 44
ipv6 address *prefix-number* 45
ipv6 extension-header drop enable 46
ipv6 hop-limit 46
ipv6 hoplimit-expires enable 47
ipv6 icmpv6 error-interval 48
ipv6 icmpv6 multicast-echo-reply enable 48
ipv6 icmpv6 source 49
ipv6 mtu 50
ipv6 nd autoconfig managed-address-flag 50
ipv6 nd autoconfig other-flag 51
ipv6 nd dad attempts 52
ipv6 nd mode uni 52
ipv6 nd ns retrans-timer 54
ipv6 nd nud reachable-time 55
ipv6 nd ra dns search-list 56
ipv6 nd ra dns search-list suppress 57
ipv6 nd ra dns server 58
ipv6 nd ra dns server suppress 59
ipv6 nd ra halt 60
ipv6 nd ra hop-limit unspecified 61
ipv6 nd ra interval 61
ipv6 nd ra invalid-delegated-prefix advertise enable 62
ipv6 nd ra no-advlinkmtu 63
ipv6 nd ra prefix 64
ipv6 nd ra router-lifetime 65
ipv6 nd router-preference 65
ipv6 nd snooping enable global 66
ipv6 nd snooping enable link-local 67
ipv6 nd snooping glean source 67
ipv6 nd snooping max-learning-num 68
ipv6 neighbor 68

ipv6 neighbor link-local minimize ····70
ipv6 neighbor stale-aging ····70
ipv6 neighbors max-learning-num ····71
ipv6 pathmtu ····75
ipv6 pathmtu age ····75
ipv6 prefer temporary-address ····76
ipv6 prefix ····77
ipv6 reassemble local enable ····78
ipv6 redirects enable ····78
ipv6 temporary-address ····79
ipv6 unreachables enable ····80
local-proxy-nd enable ····81
proxy-nd enable ····81
reset ipv6 nd snooping ····82
reset ipv6 neighbors ····82
reset ipv6 pathmtu ····83
reset ipv6 statistics ····84

IPv6 basics commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

display ipv6 fib

Use **display ipv6 fib** to display IPv6 FIB entries.

Syntax

display ipv6 fib [*ipv6-address* [*prefix-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Displays IPv6 FIB entries for a destination IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 FIB entries.

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128. If you do not specify the prefix length, this command displays the IPv6 FIB entry longest matching the IPv6 address.

Examples

Display all IPv6 FIB entries for the public network.

```
<Sysname> display ipv6 fib

Destination count: 1 FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination: ::1                                  Prefix length: 128
Nexthop    : ::1                                  Flags: UH
Time stamp : 0x1                                  Label: Null
Interface  : InLoop0                              Token: Invalid
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of IPv6 FIB entries.
Destination	Destination address.
Prefix length	Prefix length of the destination address.
Nexthop	Next hop address.

Field	Description
Flags	Route flag: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Black hole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Recursive route. • **F**—Fast re-route.
Time stamp	Time when the IPv6 FIB entry was generated.
Label	This field is not supported in the current software version. Inner MPLS label. For IPv6 FIB entries for the public network, this field displays **Null**.
Interface	Outgoing interface.
Token	Label switched path index number.

display ipv6 icmp statistics

Use **display ipv6 icmp statistics** to display ICMPv6 packet statistics.

Syntax

In standalone mode:

display ipv6 icmp statistics

In IRF mode:

display ipv6 icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMPv6 packet statistics for all member devices. (In IRF mode.)

Examples

Display ICMPv6 packet statistics.

```
<Sysname> display ipv6 icmp statistics
  Input: bad code              0         too short               0
         checksum error        0         bad length              0
         path MTU changed      0         destination unreachable 0
         too big               0         parameter problem       0
         echo request          0         echo reply              0
         neighbor solicit      0         neighbor advertisement  0
```

```
        router solicit        0         router advertisement     0
        redirect               0         router renumbering       0
output: parameter problem     0         echo request             0
        echo reply            0         unreachable no route     0
        unreachable admin     0         unreachable beyond scope 0
        unreachable address   0         unreachable no port      0
        too big               0         time exceed transit      0
        time exceed reassembly 0        redirect                 0
        ratelimited           0         other errors             0
```

Table 2 Command output

Field	Description
bad code	Number of received packets with error codes.
too short	Number of received packets with the length too short.
checksum error	Number of received packets with checksum errors.
bad length	Number of received packets with incorrect packet size.
path MTU changed	Number of received packets with path MTU changed.
destination unreachable	Number of destination unreachable packets that have been received.
too big	Number of received or sent oversized packets.
parameter problem	Number of received or sent packets with incorrect parameters.
echo request	Number of received or sent echo request packets.
echo reply	Number of received or sent echo reply packets.
neighbor solicit	Number of received NS packets.
neighbor advertisement	Number of received NA packets.
router solicit	Number of received RS packets.
router advertisement	Number of received RA packets.
redirect	Number of received or sent redirect packets.
router renumbering	Number of received packets with router renumbering.
unreachable no route	Number of sent packets to report the error that no route is available to the destination.
unreachable admin	Number of sent packets to report the error that the communication with the destination is administratively prohibited.
unreachable beyondscope	Number of sent packets to report the error that the source addresses is beyond the scope.
unreachable address	Number of address unreachable packets that have been sent.
unreachable no port	Number of port unreachable packets that have been sent.

Field	Description
time exceed transit	Number of sent packets to report the time exceeded in transmit error.
time exceed reassembly	Number of sent packets to report the fragment reassembly time exceeded error.
ratelimited	Number of packets that were not sent out because of the rate limit.
other errors	Number of sent packets with other errors.

display ipv6 interface

Use **display ipv6 interface** to display IPv6 interface information.

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

brief: Displays brief IPv6 interface information, including physical status, link-layer protocols, and IPv6 address. If you do not specify the keyword, this command displays detailed IPv6 interface information, including IPv6 configuration and operating information, and IPv6 packet statistics.

Usage guidelines

If you do not specify an interface, this command displays IPv6 information about all interfaces.

If you specify only the *interface-type* argument, this command displays IPv6 information about the interfaces of the specified type.

If you specify both the *interface-type* and the *interface-number* arguments, this command displays IPv6 information about the specified interface.

Examples

Display IPv6 information about VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
  Global unicast address(es):
    10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
    20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
    30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
    40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
```

```
    50::3, subnet is 50::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF65:4322
  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 3 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: • **Administratively DOWN**—The interface has been administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **UP**—The administrative and physical states of the interface are both up.
Line protocol current state	Link layer state of the interface: • **DOWN**—The link layer protocol state of the interface is down.

Field	Description
	• **UP**—The link layer protocol state of the interface is up.
IPv6 is enabled	IPv6 is enabled on the interface. This feature is automatically enabled after an IPv6 address is configured for an interface.
link-local address	Link-local address of the interface.
Global unicast address(es)	Global unicast addresses of the interface. IPv6 address states: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address. • **DUPLICATE**—The address is not unique on the link. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • **DEPRECATED**—The address is beyond the preferred lifetime but in the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined for the address are processed correctly. If a global unicast address is not manually configured, the following notations indicate how the address is obtained: • **AUTOCFG**—Stateless autoconfigured. • **DHCP**—Assigned by a DHCPv6 server. • **EUI-64**—Manually configured EUI-64 IPv6 address. • **RANDOM**—Random address automatically generated. If the address is a manually configured anycast address, it is noted with **ANYCAST**.
valid lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are valid.
preferred lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are preferred.
Joined group address(es)	Addresses of the multicast groups that the interface has joined.
MTU	MTU of the interface.
ND DAD is enabled, number of DAD attempts	DAD is enabled. • If DAD is enabled, this field displays the number of attempts to send an NS message for DAD (set by using the **`ipv6 nd dad attempts`** command). • If DAD is disabled, this field displays **ND DAD is disabled**. To disable DAD, set the number of attempts to 0.
ND reachable time	Time during which a neighboring device is reachable.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts obtained IPv6 addresses through stateless autoconfiguration.
InReceives	Received IPv6 packets, including error messages.
InTooShorts	Received IPv6 packets that are too short. For example, the received IPv6 packet is less than 40 bytes.
InTruncatedPkts	Received IPv6 packets with a length less than the payload length field specified in the packet header.
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the hop limit field specified in the packet header.
InBadHeaders	Received IPv6 packets with incorrect basic headers.

Field	Description
InBadOptions	Received IPv6 packets with incorrect extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of reassembled IPv6 packets.
InFragDrops	Received IPv6 fragments that are discarded because of certain errors.
InFragTimeouts	Received IPv6 fragments that are discarded because the amount of time they stay in the system buffer exceeds the specified interval.
OutFragFails	IPv6 packets that fail to be fragmented on the output interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that are delivered to user protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 user protocols.
OutForwDatagrams	IPv6 packets forwarded by the interface.
InNoRoutes	Received IPv6 packets that are discarded because no matching route can be found.
InTooBigErrors	Received IPv6 packets that fail to be forwarded because they exceeded the Path MTU.
OutFragOKs	Fragmented IPv6 packets on the output interface.
OutFragCreates	Number of IPv6 fragments on the output interface.
InMcastPkts	Received IPv6 multicast packets.
InMcastNotMembers	Received IPv6 multicast packets that are discarded because the interface is not in the multicast group.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	Received IPv6 packets that are discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that are discarded due to resource problems rather than packet errors.
OutDiscards	IPv6 packets that fail to be sent due to resource problems rather than packet errors.

Display brief IPv6 information about all interfaces.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                          Physical Protocol IPv6 Address
Vlan-interface1                    down     down     Unassigned
Vlan-interface2                    up       up       2001::1
Vlan-interface100                  up       up       Unassigned
```

Table 4 Command output

Field	Description
*down: administratively down	The interface has been administratively shut down by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.

Field	Description
Interface	Name of the interface.
Physical	Physical state of the interface: • ***down**—The interface has been administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down. The VLAN of the interface does not have ports in up state, possibly because of a connection or link failure. • **up**—The administrative and physical states of the interface are both up.
Protocol	Link layer protocol state of the interface: • **down**—The network layer protocol state of the interface is down. • **up**—The network layer protocol state of the interface is up.
IPv6 Address	IPv6 address of the interface. • If multiple global unicast addresses are configured, this field displays the lowest address. • If no global unicast address is configured, this field displays the link-local address. • If no address is configured, this field displays **Unassigned**.

display ipv6 interface prefix

Use **display ipv6 interface prefix** to display IPv6 prefix information for an interface.

Syntax

display ipv6 interface *interface-type interface-number* **prefix**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

Examples

Display IPv6 prefix information for VLAN-interface 10.

```
<Sysname> display ipv6 interface vlan-interface10 prefix
Prefix: 1001::/65                                   Origin: ADDRESS
Age:    -                                            Flag:   AL
Lifetime(Valid/Preferred): 2592000/604800

Prefix: 2001::/64                                   Origin: STATIC
Age:    -                                            Flag:   L
Lifetime(Valid/Preferred): 3000/2000

Prefix: 3001::/64                                   Origin: RA
Age:    600                                          Flag:   A
```

```
Lifetime(Valid/Preferred): -
```

Table 5 Command output

Filed	Description
Prefix	IPv6 address prefix.
Origin	How the prefix is generated: • **STATIC**—Manually configured by using the **ipv6 nd ra prefix** command. • **RA**—Advertised in RA messages after stateless autoconfiguration is enabled. • **ADDRESS**—Generated by a manually configured address.
Age	Aging time in seconds. If the prefix does not age out, this field displays a hyphen (-).
Flag	Flags carried in RA messages. If no flags are available, this field displays a hyphen (-). • **L**—The address with the prefix is directly reachable on the link. • **A**—The prefix is used for stateless autoconfiguration.
Lifetime	Lifetime in seconds advertised in RA messages. If the prefix does not need to be advertised, this field displays a hyphen (-). • **Valid**—Valid lifetime of the prefix. • **Preferred**—Preferred lifetime of the prefix.

Related commands

ipv6 nd ra prefix

display ipv6 nd snooping

Use **display ipv6 nd snooping** to display IPv6 ND snooping entries.

Syntax

display ipv6 nd snooping [[**vlan** *vlan-id* | **interface** *interface-type interface-number*] [**global** | **link-local**] | *ipv6-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Displays ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

interface *interface-type interface-number*: Displays ND snooping entries for the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number.

ipv6-address: Displays the ND snooping entry for the specified IPv6 address.

global: Displays ND snooping entries for global unicast addresses.

link-local: Displays ND snooping entries for link-local addresses.

verbose: Displays detailed information about ND snooping entries. If you do not specify the keyword, this command displays brief information about ND snooping entries.

Examples

Display IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1
IPv6 address            MAC address    VID  Interface    Status      Age
1::2                    0000-1234-0c01  1   GE1/0/2      VALID       57
```

Display detailed information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1 verbose
IPv6 address: 1::2
MAC address: 0000-1234-0c01
Interface: GE1/0/2
First VLAN ID: 1   Second VLAN ID: N/A
Status: VALID   Age: 57
```

Table 6 Command output

Filed	Description
IPv6 address	IPv6 address in the ND snooping entry.
MAC address	MAC address in the ND snooping entry.
VID	ID of the VLAN to which the ND snooping entry belongs.
First VLAN ID	ID of the SVLAN to which the ND snooping entry belongs.
Second VLAN ID	ID of the CVLAN to which the ND snooping entry belongs. If no CVLAN is configured, this field displays **N/A**.
Interface	Input interface in the ND snooping entry.
Status	Status of the ND snooping entry: • **TENTATIVE**—The entry is ineffective. • **VALID**—The entry is effective. • **TESTING TPLT**—The entry is being tested by DAD. The device performs DAD for the entry in the following situations: ○ The entry ages out ○ An ND trusted interface in the VLAN receives an ND message from the IPv6 address in the entry. • **TESTING VP**—The entry is being tested by DAD. The device performs DAD when an ND untrusted interface in the VLAN receives an ND message from the IPv6 address in the entry.
Age	For an ND snooping entry in VALID status, this field displays its remaining aging time in seconds. For an ND snooping entry in other status, this field displays a pound sign (#).

display ipv6 nd snooping count

Use **display ipv6 nd snooping count** to display the number of IPv6 ND snooping entries.

Syntax

display ipv6 nd snooping count [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the total number of ND snooping entries.

Examples

Display the total number of IPv6 ND snooping entries.

```
<Sysname> display ipv6 nd snooping count
Total number of entries: 5
```

Display the total number of IPv6 ND snooping entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd snooping count interface gigabitethernet 1/0/1
Total number of entries on interface: 2
```

display ipv6 neighbors

Use **display ipv6 neighbors** to display IPv6 neighbor information.

Syntax

In standalone mode:

display ipv6 neighbors { *ipv6-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id* } [**verbose**]

In IRF mode:

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the IPv6 address of a neighbor whose information is displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 neighbor information for all member devices. (In IRF mode.)

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

vlan *vlan-id*: Displays information about neighbors in the specified VLAN. The value range for VLAN ID is 1 to 4094.

verbose: Displays detailed neighbor information.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 address                Link layer    VID  Interface     State T  Age
FE80::200:5EFF:FE32:B800    0000-5e32-b800 N/A  GE1/0/1       REACH D  10
```

Display detailed information about all neighbors.

```
<Sysname> display ipv6 neighbors all verbose
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 Address: FE80::200:5EFF:FE32:B800
Link Layer  : 0000-5e32-b800     VID : N/A  Interface: GE1/0/1
State       : REACH              Type: IS   Age     : -
Vpn-instance: No Vrf
Nickname    : 0x0
```

Table 7 Command output

Field	Description
IPv6 Address	IPv6 address of the neighbor.
Link Layer	Link layer address (MAC address) of the neighbor.
VID	VLAN or virtual switch instance (VSI) to which the interface connected to a neighbor belongs.
Interface	Interface connected to the neighbor.
State	State of the neighbor: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • **PROBE**—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Neighbor information type: • **Static**—Statically configured. • **Dynamic**—Dynamically obtained. • **O**—Learned from the OpenFlow module. This field is not supported in the current software version. • **R**—Learned from the Portal module. • **Invalid**—Invalid.
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).
Vpn-instance	This field is not supported in the current software version. Name of a VPN or **[No Vrf]** with no VPN configured.

Field	Description
Nickname	This field is not supported in the current software version. Nickname of a neighbor entry. The name is a string of four hexadecimal numbers.

Related commands

ipv6 neighbor

reset ipv6 neighbors

display ipv6 neighbors count

Use **display ipv6 neighbors count** to display the number of neighbor entries.

Syntax

In standalone mode:

display ipv6 neighbors { { **all** | **dynamic** | **static** } | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

In IRF mode:

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries created dynamically and configured statically.

dynamic: Displays the total number of neighbor entries created dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of neighbor entries for all member devices. (In IRF mode.)

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

vlan *vlan-id*: Displays the total number of neighbor entries in the specified VLAN. The value range for VLAN ID is 1 to 4094.

Examples

Display the total number of neighbor entries created dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
 Total number of dynamic entries: 2
```

display ipv6 pathmtu

Use the **display ipv6 pathmtu** command to display IPv6 Path MTU information.

Syntax

display ipv6 pathmtu { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the destination IPv6 address for which the Path MTU information is to be displayed.

all: Displays all Path MTU information for the public network.

dynamic: Displays all dynamic Path MTU information.

static: Displays all static Path MTU information.

count: Displays the total number of Path MTU entries.

Examples

Display all Path MTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 destination address             PathMTU   Age   Type
1:2::3:2                             1800      -     Static
1:2::4:2                             1400      10    Dynamic
1:2::5:2                             1280      10    Dynamic
```

Displays the total number of Path MTU entries.

```
<Sysname> display ipv6 pathmtu all count
Total number of entries: 3
```

Table 8 Command output

Field	Description
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a Path MTU to live. For a static Path MTU, this field displays a hyphen (-).
Type	Path MTU type: • **Dynamic**—Dynamically negotiated. • **Static**—Statically configured.
Total number of entries	Total number of Path MTU entries.

Related commands

ipv6 pathmtu

reset ipv6 pathmtu

display ipv6 prefix

Use **display ipv6 prefix** to display information about IPv6 prefixes, including dynamic and static prefixes.

Syntax

display ipv6 prefix [*prefix-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-number: Specifies the ID of an IPv6 prefix, in the range of 1 to 1024. If you do not specify an IPv6 prefix ID, this command displays information about all IPv6 prefixes.

Usage guidelines

A static IPv6 prefix is configured by using the **ipv6 prefix** command.

A dynamic IPv6 prefix is obtained from the DHCPv6 server, and its prefix ID is configured by using the **ipv6 dhcp client pd** command. For more information about prefix generation, see DHCPv6 client configuration in *Network Connectivity Configuration Guide* .

Examples

Display information about all IPv6 prefixes.

```
<Sysname> display ipv6 prefix
Number  Prefix                                  Type
1       1::/16                                  Static
2       11:77::/32                              Dynamic
```

Display information about the IPv6 prefix with prefix ID 1.

```
<Sysname> display ipv6 prefix 1
Number: 1
Type  : Dynamic
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec
```

Table 9 Command output

Field	Description
Number	Prefix ID.
Type	Prefix type: • **Static**—Static IPv6 prefix. • **Dynamic**—Dynamic IPv6 prefix.
Prefix	Prefix and its length. If no prefix is obtained, this field displays **Not-available**.
Preferred lifetime 90 sec	Preferred lifetime in seconds. For a static IPv6 prefix, this field is not displayed.
valid lifetime 120 sec	Valid lifetime in seconds. For a static IPv6 prefix, this field is not displayed.

Related commands

ipv6 dhcp client pd

ipv6 prefix

display ipv6 rawip

Use **display ipv6 rawip** to display brief information about IPv6 RawIP connections.

Syntax

In standalone mode:

display ipv6 rawip

In IRF mode:

display ipv6 rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 RawIP connections for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display brief information about IPv6 RawIP connections.

```
<Sysname> display ipv6 rawip
Local Addr          Foreign Addr       Protocol PCB
2001:2002:2003:2    3001:3002:3003:3   58       0x0000000000000009
004:2005:2006:20    004:3005:3006:30
07:2008             07:3008
2002::100           2002::138          58       0x0000000000000008
::                  ::                 58       0x0000000000000002
```

(In IRF mode.) Display brief information about IPv6 RawIP connections.

```
<Sysname> display ipv6 rawip
Local Addr          Foreign Addr       Protocol Slot  PCB
2001:2002:2003:2    3001:3002:3003:3   58       1     0x0000000000000009
004:2005:2006:20    004:3005:3006:30
07:2008             07:3008
2002::100           2002::138          58       2     0x0000000000000008
::                  ::                 58       2     0x0000000000000002
```

Table 10 Command output

Field	Description
Local Addr	Local IPv6 address.
Foreign Addr	Peer IPv6 address.
Protocol	Protocol number.
PCB	PCB index.

display ipv6 rawip verbose

Use **display ipv6 rawip verbose** to display detailed information about IPv6 RawIP connections.

Syntax

In standalone mode:

display ipv6 rawip verbose [**pcb** *pcb-index*]

In IRF mode:

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 RawIP connections for all member devices. (In IRF mode.)

pcb *pcb-index*: Displays detailed information about IPv6 RawIP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

(In standalone mode.) Display detailed information about an IPv6 RawIP connection.

```
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1

 Creator: ping ipv6[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 58
 Connection info: src = ::, dst = ::
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

(In IRF mode.) Display detailed information about an IPv6 RawIP connection.

```
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1
```

```
Location: slot: 1
Creator: ping ipv6[320]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 3
Protocol: 58
Connection info: src = ::, dst = ::
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

Table 11 Command output

Field	Description
Total RawIP socket number	Total number of IPv6 RawIP sockets.
Location	Socket location.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp,

Field	Description
	accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **SO_USCBINDEX**—Obtains the user profile index from the received packets. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of protocol using the socket. 58 represents ICMP.
Connection info	Connection information, including source and destination IPv6 addresses.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag.

Field	Description
	• **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_USEICMPSRC**—Uses the specified IPv6 address as the source IPv6 address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flag in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display ipv6 statistics

Use **`display ipv6 statistics`** to display IPv6 and ICMPv6 packet statistics.

Syntax

In standalone mode:

display ipv6 statistics

In IRF mode:

display ipv6 statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 and ICMPv6 packet statistics for all member devices. (In IRF mode.)

Examples

Display IPv6 and ICMPv6 packet statistics.

```
<Sysname> display ipv6 statistics
  IPv6 statistics:

    Sent packets:
      Total:     0
        Sent locally:        0          Forwarded:            0
        Raw packets:         0          Discarded:            0
        Fragments:           0          Fragments failed:     0
        Routing failed:      0

    Received packets:
      Total:     0
        Received locally:    0          Hop limit exceeded:  0
        Fragments:           0          Reassembled:         0
        Reassembly failures:  0          Reassembly timeout:  0
        Format errors:       0          Option errors:       0
        Protocol errors:     0

  ICMPv6 statistics:

    Sent packets:
      Total:     0
        Unreachable:         0          Too big:             0
        Hop limit exceeded:  0          Reassembly timeouts: 0
        Parameter problems:  0
        Echo requests:       0          Echo replies:        0
        Neighbor solicits:   0          Neighbor adverts:    0
        Router solicits:     0          Router adverts:      0
        Redirects:           0          Router renumbering:  0
      Send failed:
        Rate limitation:     0          Other errors:        0
```

```
Received packets:
  Total:     0
    Checksum errors:     0          Too short:           0
    Bad codes:           0
    Unreachable:         0          Too big:             0
    Hop limit exceeded:  0          Reassembly timeouts:  0
    Parameter problems:  0          Unknown error types:  0
    Echo requests:       0          Echo replies:        0
    Neighbor solicits:   0          Neighbor adverts:    0
    Router solicits:     0          Router adverts:      0
    Redirects:           0          Router renumbering:  0
    Unknown info types:  0
  Deliver failed:
    Bad length:          0
```

Table 12 Command output

Field	Description
IPv6 statistics:	IPv6 packet statistics.
Sent packets: Total: Sent locally: Forwarded: Raw packets: Discarded: Fragments: Fragments failed: Routing failed:	Statistics for sent IPv6 packets: • **Total**—Total number of packets that have been locally sent and forwarded. • **Sent locally**—Number of locally sent packets. • **Forwarded**—Number of forwarded packets. • **Raw packets**—Number of packets sent by using a raw socket. • **Discarded**—Number of discarded packets. • **Fragments**—Number of sent fragments. • **Fragments failed**—Number of fragments that were failed to send. • **Routing failed**—Number of packets with routing failures.
Received packets: Total: Received locally: Hop limit exceeded: Fragments: Reassembled: Reassembly failures: Reassembly timeout: Format errors: Option errors: Protocol errors:	Statistics for received IPv6 packets: • **Total**—Total number of received packets. • **Received locally**—Number of received packets that are destined for the device. • **Hop limit exceeded**—Number of packets with hop limit exceeded. • **Fragments**—Number of received fragments. • **Reassembled**—Number of reassembled packets. • **Reassembly failures**—Number of packets with reassembly failures. • **Reassembly timeout**—Number of packets with reassembly timed out. • **Format errors**—Number of packets with format errors. • **Option errors**—Number of packets with option errors. • **Protocol errors**—Number of packets with protocol errors.
ICMPv6 statistics:	ICMPv6 message statistics.

Field	Description
Sent packets: Total: Unreached: Too big: Hop limit exceeded: Reassembly timeouts: Parameter problems: Echo requests: Echo replies: Neighbor solicits: Neighbor adverts: Router solicits: Router adverts: Redirects: Router renumbering Sent failed: Rate limitation: Other errors:	Statistics for sent ICMPv6 messages: • **Total**—Total number of sent messages. • **Unreached**—Number of Destination Unreachable messages. This field is not supported in the current software version. • **Too big**—Number of Packet Too Big messages. • **Hop limit exceeded**—Number of Hop Limit Exceeded messages. • **Reassembly timeouts**—Number of Fragment Reassembly Time Exceeded messages. • **Parameter problems**—Number of Parameter Problem messages. • **Echo requests**—Number of Echo Requests. • **Echo replies**—Number of Echo Replies. • **Neighbor solicits**—Number of Neighbor Solicitation messages. • **Neighbor adverts**—Number of Neighbor Advertisement messages. • **Router solicits**—Number of Router Solicitation messages. • **Router adverts**—Number of Router Advertisement messages. • **Redirects**—Number of Redirect messages. • **Router renumbering**—Number of Router Renumbering messages. This field is not supported in the current software version. • **Sent failed**—Number of messages that were failed to send locally. • **Rate limitation**—Number of unsent messages because of rate limiting. • **Other errors**—Number of messages with other errors.
Received packets: Total: Checksum errors: Too short: Bad codes: Unreachable: Too big: Hop limit exceeded: Reassembly timeouts: Parameter problems: Unknown error types: Echo requests: Echo replies: Neighbor solicits: Neighbor adverts: Router solicits: Router adverts:	Statistics for received ICMPv6 messages: • **Total**—Total number of received messages. • **Checksum errors**—Number of messages with checksum errors. • **Too short**—Number of messages with a too short length. • **Bad codes**—Number of messages with error codes. • **Unreached**—Number of Destination Unreachable messages. • **Too big**—Number of Packet Too Big messages. • **Hop limit exceeded**—Number of Hop Limit Exceeded messages. • **Reassembly timeouts**—Number of Fragment Reassembly Time Exceeded messages. • **Parameter problems**—Number of Parameter Problem messages. • **Unknown error types**—Number of messages with unknown error types.

Field	Description
Redirects: Router renumbering: Unknown info types: Deliver failed: Bad length:	• **Echo requests**—Number of Echo Requests. • **Echo replies**—Number of Echo Replies. • **Neighbor solicits**—Number of Neighbor Solicitation messages. • **Neighbor adverts**—Number of Neighbor Advertisement messages. • **Router solicits**—Number of Router Solicitation messages. • **Router adverts**—Number of Router Advertisement messages. • **Redirects**—Number of Redirect messages. **Router renumbering**—Number of Router Renumbering messages. This field is not supported in the current software version. • **Unknown info types**—Number of messages with unknown information types. • **Deliver failed**—Number of messages with local delivery failures. • **Bad length**—Number of messages with error length.

Related commands

reset ipv6 statistics

display ipv6 tcp

Use **display ipv6 tcp** to display brief information about IPv6 TCP connections.

Syntax

In standalone mode:

display ipv6 tcp

In IRF mode:

display ipv6 tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 TCP connections for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Display brief information about IPv6 TCP connections.

```
<Sysname> display ipv6 tcp
*: TCP MD5 Connection
```

```
 LAddr->port        FAddr->port      State       PCB
*2001:2002:2003:2   3001:3002:3003:3 ESTABLISHED 0x000000000000c387
004:2005:2006:20    004:3005:3006:30
07:2008->1200       07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED 0x0000000000000008
2003::1->25         2001::2->1283    LISTEN      0x0000000000000009
```

(In IRF mode.) Display brief information about IPv6 TCP connections.

```
<Sysname> display ipv6 tcp
*: TCP MD5 Connection
 LAddr->port        FAddr->port      State       Slot  PCB
*2001:2002:2003:2   3001:3002:3003:3 ESTABLISHED 1     0x000000000000c387
004:2005:2006:20    004:3005:3006:30
07:2008->1200       07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED 1     0x0000000000000008
2003::1->25         2001::2->1283    LISTEN      1     0x0000000000000009
```

Table 13 Command output

Field	Description
*	Indicates that the TCP connection uses MD5 authentication.
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **IME_WAIT**—The client receives a disconnection request from the server.
PCB	PCB index.

display ipv6 tcp verbose

Use **display ipv6 tcp verbose** to display detailed information about IPv6 TCP connections.

Syntax

In standalone mode:

display ipv6 tcp verbose [**pcb** *pcb-index*]

In IRF mode:

display ipv6 tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 TCP connections for all member devices. (In IRF mode.)

pcb *pcb-index*: Displays detailed information about IPv6 TCP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

(In standalone mode.) Display detailed information about an IPv6 TCP connection.

```
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65536 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
 Type: 1
 Protocol: 6
 Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

(In IRF mode.) Display detailed information about an IPv6 TCP connection.

```
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Location: Slot: 1
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65536 / 1 / 0 / N/A
```

```
Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
Type: 1
Protocol: 6
Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

Table 14 Command output

Field	Description
TCP inpcb number	Number of IPv6 TCP Internet PCBs.
tcpcb number	Number of IPv6 TCP PCBs (excluding PCBs of TCP in TIME_WAIT state).
Location	Socket location.
NSR standby	ID of the IRF member device and number of the slot where the NSR standby card resides. This field displays **N/A** if no NSR standby card is present.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated.

Field	Description
	• **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 6 represents TCP.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP

Field	Description
	and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXLISTEN**—Listening socket. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Connection state	TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request.

Field	Description
	• **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_PASSWORD**—The MD5 password is configured. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option.
NSR state	NSR state of the TCP connection: • **CLOSED**—Closed (initial) state. • **CLOSING**—The connection is to be closed. • **ENABLED**—The connection backup is enabled. • **OPEN**—The connection synchronization has started. • **PENDING**—The connection backup is not ready. • **READY**—The connection backup is ready. • **SMOOTH**—The connection data is being smoothed. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display ipv6 tcp-proxy

Use **display ipv6 tcp-proxy** to display brief information about IPv6 TCP proxy.

Syntax

In standalone mode:

display ipv6 tcp-proxy

In IRF mode:

display ipv6 tcp-proxy slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: • WX2508H-PWR-LTE • WX2540H • WX2540H-F • WX2560H No: • WX2510H-PWR • WX2510H-F-PWR
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3010H-X-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes: WX5510E No: WX5540E
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR	Yes

Hardware series	Model	Product code	Command compatibility
	WX1810H-PWR WX1820H WX1840H	EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Examples

Display brief information about IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy slot 1
LAddr->port          FAddr->port           State       Service type
2001::1->45          11:22:33:44->54602    ESTABLISHED NONE
11:22:33:44->54602   2001::1->45           ESTABLISHED NONE
```

Table 15 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.
Faddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RECEIVED**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
Service type	Type of services that the IPv6 TCP proxy is used for: • **NONE**—No service type is specified. •

display ipv6 tcp-proxy port-info

Use **display ipv6 tcp-proxy port-info** to display the usage of non-well known ports for IPv6 TCP proxy.

Syntax

In standalone mode:

display ipv6 tcp-proxy port-info

In IRF mode:

display ipv6 tcp-proxy port-info slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes: • WX2508H-PWR-LTE • WX2540H • WX2540H-F • WX2560H No: • WX2510H-PWR • WX2510H-F-PWR
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3010H-X-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes: WX5510E No: WX5540E
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No

Hardware series	Model	Product code	Command compatibility
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays non-well known port usage for all member devices. (In IRF mode.)

Usage guidelines

The TCP ports are divided into well-known ports (port numbers from 0 through 1023) and non-well known ports (port numbers from 1024 through 65535).

- Well known ports are for certain services, for example, port 23 for Telnet service, ports 20 and 21 for FTP service, and port 80 for HTTP service.
- Non-well known ports are available for various services. You can use the **display ipv6 tcp-proxy port-info** command to display the usage of these ports.

Examples

Display the usage of non-well known ports for IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy port-info
Index  Range          State
16     [1024, 1087]    USABLE
17     [1088, 1151]    USABLE
18     [1152, 1215]    USABLE
19     [1216, 1279]    USABLE
20     [1280, 1343]    USABLE
```

```
...
1020   [65280, 65343]   USABLE
1021   [65344, 65407]   USABLE
1022   [65408, 65471]   USABLE
1023   [65472, 65535]   USABLE
```

Table 16 Command output

Field	Description
Index	Index of the port range.
Range	Start port number and end port number.
State	State of the port range: • **USABLE**—The ports are assignable. • **ASSIGNED**—Some ports are dynamically assigned and some ports are not. • **ALLASSIGNED**—All ports are dynamically assigned. The assigned ports can be reclaimed. • **TO RECLAIM**—Some ports are statically assigned. The assigned ports can be reclaimed. • **RESERVED**—The ports are reserved. The reserved ports cannot be dynamically assigned.

display ipv6 udp

Use **display ipv6 udp** to display brief information about IPv6 UDP connections.

Syntax

In standalone mode:

display ipv6 udp

In IRF mode:

display ipv6 udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 UDP connections for all member devices. (In IRF mode.)

Examples

(In standalone mode.) Displays brief information about IPv6 UDP connections.

```
<Sysname> display ipv6 udp
 LAddr->port        FAddr->port        PCB
 2001:2002:2003:2   3001:3002:3003:3   0x000000000000c387
 004:2005:2006:20   004:3005:3006:30
 07:2008->1200      07:3008->1200
```

```
 2001::1->23        2001::5->1284      0x0000000000000008
 2003::1->25        2001::2->1283      0x0000000000000009
```

(In IRF mode.) Displays brief information about IPv6 UDP connections.

```
<Sysname> display ipv6 udp
 LAddr->port        FAddr->port        Slot  PCB
 2001:2002:2003:2   3001:3002:3003:3   1     0x000000000000c387
 004:2005:2006:20   004:3005:3006:30
 07:2008->1200      07:3008->1200
 2001::1->23        2001::5->1284      1     0x0000000000000008
 2003::1->25        2001::2->1283      1     0x0000000000000009
```

Table 17 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
PCB	PCB index.

display ipv6 udp verbose

Use **display ipv6 udp verbose** to display detailed information about IPv6 UDP connections.

Syntax

In standalone mode:

display ipv6 udp verbose [**pcb** *pcb-index*]

In IRF mode:

display ipv6 udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 UDP connections for all member devices. (In IRF mode.)

pcb *pcb-index*: Displays detailed information about IPv6 UDP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

(In standalone mode.) Display detailed information about an IPv6 UDP connection.

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

 Creator: sock_test_mips[250]
 State: N/A
```

```
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = ::->69, dst = ::->0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

(In IRF mode.) Display detailed information about an IPv6 UDP connection.

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

 Location: slot: 1
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = ::->69, dst = ::->0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 18 Command output

Field	Description
Total UDP socket number	Total number of IPv6 UDP sockets.
Location	Socket location.
Creator	Task name of the socket. The progress number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.

Field	Description
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the

Field	Description
	next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 17 represents UDP.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB.

Field	Description
	• **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

ipv6 address

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to delete an IPv6 global unicast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

Default

No IPv6 global unicast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Usage guidelines

Like public IPv4 addresses, IPv6 global unicast addresses are assigned to ISPs. This type of address allows for prefix aggregation to reduce the number of global routing entries.

If you do not specify any parameters, the **undo ipv6 address** command deletes all IPv6 addresses of an interface.

Examples

Set the IPv6 global unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

ipv6 address anycast

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to delete the IPv6 anycast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

Default

No IPv6 anycast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 anycast address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Examples

Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 anycast
```

ipv6 address auto

Use **ipv6 address auto** to enable the stateless address autoconfiguration feature on an interface, so that the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this feature.

Syntax

ipv6 address auto

undo ipv6 address auto

Default

The stateless address autoconfiguration feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically.

To delete the global unicast address and the link-local address that are automatically generated, use either of the following commands:

- **undo ipv6 address auto**
- **undo ipv6 address**

Examples

Enable stateless address autoconfiguration on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto
```

ipv6 address auto link-local

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to restore the default.

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

Default

No link-local address is configured on an interface. A link-local address is automatically generated after an IPv6 global unicast address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Link-local addresses are used for neighbor discovery and stateless autoconfiguration on the local link. Packets using link-local addresses as the source or destination addresses cannot be forwarded to other links.

After an IPv6 global unicast address is configured for an interface, a link-local address is automatically generated. This link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.

The **undo ipv6 address auto link-local** command deletes only the link-local addresses generated through the **ipv6 address auto link-local** command. If the **undo** command is executed on an interface with an IPv6 global unicast address configured, the interface still has a link-local address.

You can also manually assign an IPv6 link-local address for an interface by using the **ipv6 address link-local** command. Manual assignment takes precedence over automatic generation for IPv6 link-local addresses.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated address.
- If you first use manual assignment and then automatic generation, both of the following occur:
  - The automatically generated link-local address does not take effect.
  - The link-local address of an interface is still the manually assigned address.

  If you delete the manually assigned address, the automatically generated link-local address takes effect.

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
```

Related commands

ipv6 address link-local

ipv6 address eui-64

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to delete an EUI-64 IPv6 address from an interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

Default

No EUI-64 IPv6 address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address prefix-length: Specifies an IPv6 address and IPv6 prefix length. The *ipv6-address* and *prefix-length* arguments specify the prefix of an EUI-64 IPv6 address. The value range for the *prefix-length* argument is 1 to 64. The IPv6 address and IPv6 prefix length support the following formats:

- *ipv6-address/prefix-length*. For example: 2001::1/64.
- *ipv6-address prefix-length*. For example: 2001::1 64.

Usage guidelines

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface ID. To display the EUI-64 IPv6 address, use the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot be greater than 64.

Examples

Configure an EUI-64 IPv6 address for VLAN-interface 100. The prefix of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 eui-64
```

Related commands

display ipv6 interface

ipv6 address link-local

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to restore the default.

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Default

No link-local address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Usage guidelines

Manual assignment takes precedence over automatic generation.

If you use automatic generation, and then use manual assignment, the manually assigned link-local address overwrites the one that is automatically generated.

If you use manual assignment and then use automatic generation, both of the following occur:

- The automatically generated link-local address does not take effect.
- The manually assigned link-local address of an interface remains.

After you delete the manually assigned address, the automatically generated link-local address takes effect. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

Related commands

ipv6 address auto link-local

ipv6 address *prefix-number*

Use **ipv6 address** *prefix-number* to specify an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertise the prefix.

Use **undo ipv6 address** *prefix-number* to restore the default.

Syntax

ipv6 address *prefix-number sub-prefix/prefix-length*

undo ipv6 address *prefix-number*

Default

No IPv6 prefix is specified for IPv6 address autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies an IPv6 prefix by its ID in the range of 1 to 1024. The specified IPv6 prefix can be manually configured or obtained through DHCPv6.

sub-prefix: Specifies the sub-prefix bit and host bit for the IPv6 global unicast address.

prefix-length: Specifies the sub-prefix length in the range of 1 to 128.

Usage guidelines

This command enables an interface to automatically generate an IPv6 global unicast address based on the specified IPv6 prefix, sub-prefix bit, and host bit.

An interface can generate only one IPv6 global unicast address based on the prefix specified by using the **ipv6 address** command. To configure the interface to generate a new IPv6 address, execute the **undo ipv6 address** command to delete the configuration, and then execute the **ipv6 address** command.

Examples

Configure a static IPv6 prefix AAAA::/16 and assign ID 1 to the prefix. Configure VLAN-interface 100 to use this prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise this prefix.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

Configure VLAN-interface 10 to obtain an IPv6 prefix through DHCPv6 and assign ID 2 to the obtained prefix. Configure VLAN-interface 100 to use the obtained prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise the prefix.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 2 rapid-commit option-group 1
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2 BBBB:CCCC:DDDD::10/32
```

Related commands

ipv6 prefix

ipv6 dhcp client pd

ipv6 extension-header drop enable

Use **ipv6 extension-header drop enable** to enable a device to discard IPv6 packets that contain extension headers.

Use **undo ipv6 extension-header drop enable** to disable a device from discarding IPv6 packets that contain extension headers.

Syntax

ipv6 extension-header drop enable

undo ipv6 extension-header drop enable

Default

A device does not discard IPv6 packets that contain extension headers.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to discard a received IPv6 packet in which the extension headers cannot be processed by the device.

Examples

Enable the device to discard IPv6 packets that contain extension headers.

```
<Sysname> system-view
[Sysname] ipv6 extension-header drop enable
```

ipv6 hop-limit

Use **ipv6 hop-limit** to set the Hop Limit field in the IPv6 header.

Use **undo ipv6 hop-limit** to restore the default.

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

Default

The hop limit is 64.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the number of hops, in the range of 1 to 255.

Usage guidelines

The hop limit determines the number of hops that an IPv6 packet generated by the device can travel.

The device advertises the hop limit in RA messages. All RA message receivers use the advertised value to fill in the Hop Limit field for IPv6 packets to be sent. To disable the device from advertising the hop limit, use the **ipv6 nd ra hop-limit unspecified** command.

Examples

Set the maximum number of hops to 100.

```
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

Related commands

ipv6 nd ra hop-limit unspecified

ipv6 hoplimit-expires enable

Use **ipv6 hoplimit-expires enable** to enable sending ICMPv6 time exceeded messages.

Use **undo ipv6 hoplimit-expires** to disable sending ICMPv6 time exceeded messages.

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires enable

Default

Sending ICMPv6 time exceeded messages is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMPv6 time exceeded messages are sent to the source of IPv6 packets after the device discards IPv6 packets because hop or reassembly times out.

To prevent too many ICMPv6 error messages from affecting device performance, disable this feature. Even with the feature disabled, the device still sends fragment reassembly time exceeded messages.

Examples

Disable sending ICMPv6 time exceeded messages.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires enable
```

ipv6 icmpv6 error-interval

Use **ipv6 icmpv6 error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMPv6 error messages.

Use **undo ipv6 icmpv6 error-interval** to restore the default.

Syntax

ipv6 icmpv6 error-interval *interval* [*bucketsize*]

undo ipv6 icmpv6 error-interval

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMPv6 rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMPv6 error messages are sent. Use this command to prevent network congestion caused by excessive ICMPv6 error messages generated within a short period. A token bucket algorithm is used with one token representing one ICMPv6 error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMPv6 error message is sent. When the bucket is empty, ICMPv6 error messages are not sent until a new token is placed in the bucket.

Examples

Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMPv6 error messages.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 error-interval 200 40
```

ipv6 icmpv6 multicast-echo-reply enable

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to restore the default.

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply enable

Default

The device is disabled from replying to multicast echo requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If a host is configured to reply to multicast echo requests, an attacker can use this mechanism to attack the host. For example, the attacker can send an echo request to a multicast address with Host A as the source. All hosts in the multicast group will send echo replies to Host A.

To prevent attacks, do not enable the device to reply to multicast echo requests unless necessary.

Examples

Enable replying to multicast echo requests.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 icmpv6 source

Use **ipv6 icmpv6 source** to specify an IPv6 address as the source address for outgoing ICMPv6 packets.

Use **undo ipv6 icmpv6 source** to remove the specified IPv6 source address for outgoing ICMPv6 packets.

Syntax

ipv6 icmpv6 source *ipv6-address*

undo ipv6 icmpv6 source

Default

No IPv6 source address for outgoing ICMPv6 packets is specified. The device uses the IPv6 address of the sending interface as the source IPv6 address for outgoing ICMPv6 packets.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

Usage guidelines

It is a good practice to specify the IPv6 address of the loopback interface as the source IPv6 address for outgoing ping echo request and ICMPv6 error messages. This feature helps users to easily locate the sending device.

Examples

Specify IPv6 address 1::1 as the source address for outgoing ICMPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 source 1::1
```

ipv6 mtu

Use **ipv6 mtu** to configure the interface MTU for IPv6 packets.

Use **undo ipv6 mtu** to restore the default MTU.

Syntax

ipv6 mtu *size*

undo ipv6 mtu

Default

The interface MTU is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU size in bytes.

Usage guidelines

IPv6 routers do not support packet fragmentation. After an IPv6 router receives an IPv6 packet, if the packet size is larger than the MTU of the forwarding interface, the router discards the packet. Meanwhile, the router sends the MTU to the source host through an ICMPv6 packet — Packet Too Big message. The source host fragments the packet according to the MTU and resends it. To reduce the extra flow overhead resulting from packet drops, set an appropriate interface MTU for your network.

Examples

Set the interface MTU for IPv6 packets to 1280 bytes on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Default

The M flag is set to **0** in RA advertisements. Hosts receiving the advertisements will obtain IPv6 addresses through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The M flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain IPv6 addresses.

- If the M flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from an DHCPv6 server) to obtain IPv6 addresses.
- If the M flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration. Stateless autoconfiguration generates IPv6 addresses according to link-layer addresses and the prefix information in the RA advertisements.

Examples

Set the M flag to 1 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Default

The O flag is set to **0** in RA advertisements. Hosts receiving the advertisements will acquire other information through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The O flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain configuration information other than IPv6 addresses.

- If the O flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 addresses.
- If the O flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration to obtain configuration information other than IPv6 addresses.

Examples

Set the O flag to 0 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Use **ipv6 nd dad attempts** to set the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

Syntax

ipv6 nd dad attempts *interval*

undo ipv6 nd dad attempts

Default

The number of attempts to send an NS message for DAD is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. If it is set to 0, DAD is disabled.

Usage guidelines

An interface sends an NS message for DAD after obtaining an IPv6 address.

If the interface does not receive a response within the time specified by using **ipv6 nd ns retrans-timer**, it resends an NS message.

If the interface receives no response after making the maximum sending attempts, the interface uses the obtained address.

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
```

Related commands

display ipv6 interface

ipv6 nd ns retrans-timer

ipv6 nd mode uni

Use **ipv6 nd mode uni** to configure a port as a customer-side port.

Use **undo ipv6 nd mode** to restore the default.

Syntax

ipv6 nd mode uni

undo ipv6 nd mode

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-L-PWR • WX3024H-PWR • WX3024H-F • WX3024H-L No: WX3010H-X-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Default

A port acts as a network-side port.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

By default, the device associates an ND entry with routing information when the device learns an ND entry. The ND entry provides the next hop information for routing. To save hardware resources, you can use this command to specify a port that connects to a user terminal as a customer-side port. The device will not associate the routing information with the learned ND entries.

Examples

Specify VLAN-interface 2 as a customer-side port.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 nd mode uni
```

ipv6 nd ns retrans-timer

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

Default

The local interface sends NS messages at every an interval of 1000 milliseconds, and the Retrans Timer field in the RA messages sent is 0. The interval for retransmitting an NS message is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the interval value in the range of 1000 to 4294967295 milliseconds.

Usage guidelines

If a device does not receive a response from the peer within the specified interval, the device resends an NS message. The device retransmits an NS message at the specified interval and uses the interval value to fill the Retrans Timer field in RA messages to be sent.

Examples

Specify VLAN-interface 100 to retransmit NS messages every 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

Related commands

display ipv6 interface

ipv6 nd nud reachable-time

Use **ipv6 nd nud reachable-time** to set the neighbor reachable time on an interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

Syntax

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

Default

The neighbor reachable time on the local interface is 30000 milliseconds, and the value of the Reachable Time field in RA messages is 0. The reachable time is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the neighbor reachable time in the range of 1 to 3600000 milliseconds.

Usage guidelines

If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device must send a packet to the neighbor after the specified reachable time expires, the device reconfirms whether the neighbor is reachable. The device sets the specified value as the neighbor reachable time on the local interface and uses the value to fill the Reachable Time field in RA messages to be sent.

Examples

Set the neighbor reachable time on VLAN-interface 100 to 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

Related commands

display ipv6 interface

ipv6 nd ra dns search-list

Use **ipv6 nd ra dns search-list** to specify DNS suffix information to be advertised in RA messages.

Use **undo ipv6 nd ra dns search-list** to remove a DNS suffix from RA message advertisement.

Syntax

ipv6 nd ra dns search-list *domain-name* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns search-list *domain-name*

Default

DNS suffix information is not specified and RA messages do not contain DNS suffix options.

Views

Interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a DNS suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The DNS suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

seconds: Specifies the lifetime of the DNS suffix, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS suffix is infinite.

infinite: Sets the lifetime of the DNS suffix to infinite.

seqno: Specifies the sequence number of the DNS suffix, in the range of 0 to 4294967295. The sequence number for a DNS suffix must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS search list (DNSSL) option in RA messages provides DNS suffix information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS suffixes on an interface. One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

The sequence number uniquely identifies a DNS suffix. To modify a DNS suffix or its sequence number, you must first use the **undo ipv6 nd ra dns search-list** command to remove the DNS suffix from RA message advertisement.

After you execute the **ipv6 nd ra dns search-list** command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the **undo ipv6 nd ra dns search-list** command, the device immediately sends two RA messages.

- The first RA message contains information about all DNS suffixes, including DNS suffixes specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message contains information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS suffix as **com**, the suffix lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list com infinite sequence 1
```

Related commands

ipv6 nd ra dns search-list suppress

ipv6 nd ra interval

ipv6 nd ra dns search-list suppress

Use **ipv6 nd ra dns search-list suppress** to enable DNS suffix suppression in RA messages.

Use **undo ipv6 nd ra dns search-list suppress** to disable DNS suffix suppression in RA messages.

Syntax

ipv6 nd ra dns search-list suppress

undo ipv6 nd ra dns search-list suppress

Default

DNS suffix suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS suffixes in RA messages on an interface. If you specify a new DNS suffix or remove a DNS suffix on the interface, the device immediately sends an RA message without any DNSSL options.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS suffix information configured, the device immediately sends two RA messages. In the first message, the lifetime for DNS suffixes is 0 seconds. The second RA message does not contain any DNSSL options.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Whether disabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS suffix information configured, the device immediately sends an RA message containing the DNS suffix information.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS suffix suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list suppress
```

Related commands

ipv6 nd ra dns search-list

ipv6 nd ra dns server

Use **ipv6 nd ra dns server** to specify DNS server information to be advertised in RA messages.

Use **undo ipv6 nd ra dns server** to remove a DNS server from RA message advertisement.

Syntax

ipv6 nd ra dns server *ipv6-address* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns server *ipv6-address*

Default

DNS server information is not specified and RA messages do not contain DNS server options.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the DNS server, which must be a global unicast address or a link-local address.

seconds: Specifies the lifetime of the DNS server, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS server is infinite.

infinite: Sets the lifetime of the DNS server to infinite.

sequence *seqno*: Specifies the sequence number of the DNS server, in the range of 0 to 4294967295. The sequence number for a DNS server must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS server option in RA messages provides DNS server information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS servers on an interface. One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

The sequence number uniquely identifies a DNS server. To modify the IPv6 address or sequence number of a DNS server, you must first use the **undo ipv6 nd ra dns server** command to remove the DNS server from RA message advertisement.

After you execute the **ipv6 nd ra dns server** command, the device immediately sends an RA message with the existing and newly specified DNS server options.

After you execute the **undo ipv6 nd ra dns server** command, the device immediately sends two RA messages.

- The first RA message contains information about all DNS servers, including the DNS servers specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message contains information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

In an IPv6 environment, PPP users can obtain the IPv6 DNS server address through AAA authorization. This AAA-authorized IPv6 DNS server address is also carried in RA messages. If an interface obtains the AAA-authorized and manually specified IPv6 DNS server addresses, the RA messages contain both, with the AAA-authorized address in the front. When the two addresses conflict, the AAA-authorized DNS-related attributes are used.

For more information about the PPP support for IPv6, see PPP configuration in *Network Connectivity Configuration Guide*.

Examples

Specify the DNS server address as **2001:10::100**, the server lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server 2001:10::100 infinite sequence 1
```

Related commands

ipv6 nd ra dns server suppress

ipv6 nd ra interval

ipv6 nd ra dns server suppress

Use **ipv6 nd ra dns server suppress** to enable DNS server suppression in RA messages.

Use **undo ipv6 nd ra dns server suppress** to disable DNS server suppression in RA messages.

Syntax

ipv6 nd ra dns server suppress

undo ipv6 nd ra dns server suppress

Default

DNS server suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS server addresses in RA messages on an interface. If you specify a new DNS server or remove a DNS server on the interface, the device immediately sends an RA message without any DNS server options.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS server information configured or has obtained an AAA-authorized DNS server address, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not contain any DNS server options.
- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.

Whether disabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS server information configured or has obtained an AAA-authorized DNS server address, the device immediately sends an RA message containing the DNS server information.
- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS server suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server suppress
```

Related commands

ipv6 nd ra dns server

ipv6 nd ra halt

Use **ipv6 nd ra halt** to suppress an interface from advertising RA messages.

Use **undo ipv6 nd ra halt** to disable this feature.

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

Default

An interface is suppressed from sending RA messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable RA message suppression on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd ra halt
```

ipv6 nd ra hop-limit unspecified

Use **ipv6 nd ra hop-limit unspecified** to specify unlimited hops in RA messages.

Use **undo ipv6 nd ra hop-limit unspecified** to restore the default.

Syntax

ipv6 nd ra hop-limit unspecified

undo ipv6 nd ra hop-limit unspecified

Default

The maximum number of hops in the RA messages is limited to 64.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

To set the maximum number of hops to a value rather than the default setting, use the **ipv6 hop-limit** command.

Examples

Specify unlimited hops in the RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 nd ra hop-limit unspecified
```

Related commands

ipv6 hop-limit

ipv6 nd ra interval

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages.

Use **undo ipv6 nd ra interval** to restore the default.

Syntax

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

Default

The maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-interval: Specifies the maximum interval value in seconds, in the range of 4 to 1800.

min-interval: Specifies the minimum interval value in the range of 3 seconds to three-fourths of the maximum interval.

Usage guidelines

The device advertises RA messages randomly between the maximum interval and the minimum interval.

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 1000 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
```

Related commands

ipv6 nd ra router-lifetime

ipv6 nd ra invalid-delegated-prefix advertise enable

Use **ipv6 nd ra invalid-delegated-prefix advertise enable** to enable advertising invalid delegated prefixes.

Use **undo ipv6 nd ra invalid-delegated-prefix advertise enable** to diable advertising invalid delegated prefixes.

Syntax

ipv6 nd ra invalid-delegated-prefix advertise enable

undo ipv6 nd ra invalid-delegated-prefix advertise enable

Default

Advertising invalid delegated prefixes is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

An interface can generate an IPv6 address based on a prefix, which is assigned by the DHCPv6 server. When the assigned prefix goes invalid, the device does not advertise RA messages for the event by default. In this case, endpoints that use this prefix are not aware of the event, and continue using the IPv6 addresses generated based on the prefix, causing communication failures. To avoid this problem, you can use this feature. When a DHCPv6 server-assigned prefix goes invalid, the device sends out RA messages immediately. In the message, the preferred lifetime and valid lifetime are both set to 0, announcing that the prefix is invalid. Upon receiving the advertisement, endpoints will no longer use the IPv6 addresses generated based on the prefix. For more information about DHCPv6 server, see DHCPv6 server configuration in *Network Connectivity Configuration Guide.*

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Examples

Enable advertising invalid delegated prefixes on VLAN-interface 200.

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] ipv6 nd ra invalid-delegated-prefix advertise enable
```

Related commands

ipv6 dhcp client pd

ipv6 nd ra halt

ipv6 nd ra no-advlinkmtu

Use **ipv6 nd ra no-advlinkmtu** to turn off the MTU option in RA messages.

Use **undo ipv6 nd ra no-advlinkmtu** to restore the default.

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

Default

RA messages contain the MTU option.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The MTU option in the RA messages specifies the link MTU to ensure that all nodes on the link use the same MTU.

Examples

Turn off the MTU option in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra no-advlinkmtu
```

ipv6 nd ra prefix

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to restore the default.

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-length* [**no-autoconfig** | **off-link**] * | **no-advertise**]

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix/prefix-length* }

Default

No prefix information is configured for RA messages. Instead, the IPv6 address of the interface sending RA messages is used as the prefix information.

If the IPv6 address is manually configured, the prefix uses the fixed valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (7 days).

If the IPv6 address is automatically obtained (through DHCP, for example), the prefix uses the valid and preferred lifetime of the IPv6 address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

After hosts on the same link receive RA messages, they can use the prefix information in the RA messages for stateless autoconfiguration.

Examples

Configure the prefix information in RA messages on VLAN-interface 100.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

Method 2:

```
<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

Use **ipv6 nd ra router-lifetime** to set the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

Syntax

ipv6 nd ra router-lifetime *time*

undo ipv6 nd ra router-lifetime

Default

The router lifetime in RA messages is three times as long as the maximum interval for advertising RA messages.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the router lifetime in the range of 0 to 9000 seconds. If the value is set to 0, the router does not act as the default router.

Usage guidelines

The router lifetime in RA messages specifies how long the router sending the RA messages acts as the default router. Hosts receiving the RA messages check this value to determine whether to use the sending router as the default router. If the router lifetime is 0, the router cannot be used as the default router.

The router lifetime in RA messages must be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on VLAN-interface 100 to 1000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

Related commands

ipv6 nd ra interval

ipv6 nd router-preference

Use **ipv6 nd router-preference** to set a router preference in RA messages.

Use **undo ipv6 nd router-preference** to restore the default.

Syntax

ipv6 nd router-preference { **high** | **low** | **medium** }

undo ipv6 nd router-preference

Default

The router preference is **medium**.

Views

Interface view

Predefined user roles

network-admin

Parameters

high: Sets the router preference to the highest setting.

low: Sets the router preference to the lowest setting.

medium: Sets the router preference to the medium setting.

Usage guidelines

A hosts selects a router with the highest preference as the default router.

When router preferences are the same in RA messages, a host selects the router corresponding to the first received RA message as the default gateway.

Examples

Set the router preference in RA messages to the highest on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd router-preference high
```

ipv6 nd snooping enable global

Use **ipv6 nd snooping enable global** to enable ND snooping for global unicast addresses.

Use **undo ipv6 nd snooping enable global** to disable ND snooping for global unicast addresses.

Syntax

ipv6 nd snooping enable global

undo ipv6 nd snooping enable global

Default

ND snooping is disabled for global unicast addresses.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND snooping for global unicast addresses.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable global
```

ipv6 nd snooping enable link-local

Use **ipv6 nd snooping enable link-local** to enable ND snooping for link-local addresses.

Use **undo ipv6 nd snooping enable link-local** to disable ND snooping for link-local addresses.

Syntax

ipv6 nd snooping enable link-local

undo ipv6 nd snooping enable link-local

Default

ND snooping is disabled for link-local addresses.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND snooping for link-local addresses.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable link-local
```

ipv6 nd snooping glean source

Use **ipv6 nd snooping glean source** to enable ND snooping for data packets from unknown sources.

Use **undo ipv6 nd snooping glean source** to disable ND snooping for data packets from unknown sources.

Syntax

ipv6 nd snooping glean source

undo ipv6 nd snooping glean source

Default

ND snooping is disabled for data packets from unknown sources.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to learn ND snooping entries from data packets originated by unknown sources.

For this command to take effect, execute the **ipv6 nd snooping enable global** command or the **ipv6 nd snooping enable link-local** command.

Before enabling ND snooping entries learning from data packets for a VLAN, you must configure IPv6 source guard on all untrusted interfaces in the same VLAN. This operation ensures correct forwarding of the data packets received all these interfaces.

Examples

Enable ND snooping for data packets from unknown sources.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping glean source
```

ipv6 nd snooping max-learning-num

Use **ipv6 nd snooping max-learning-num** to set the maximum number of ND snooping entries that an interface can learn.

Use **undo ipv6 nd snooping max-learning-num** to restore the default.

Syntax

ipv6 nd snooping max-learning-num *max-number*

undo ipv6 nd snooping max-learning-num

Default

An interface can learn a maximum of 2048 ND snooping entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of ND snooping entries that an interface can learn. The value range for this argument is 1 to 2048.

Examples

Allow GigabitEthernet 1/0/1 to learn a maximum of 64 ND snooping entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 64
```

ipv6 neighbor

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to delete a neighbor entry.

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*

Default

No static neighbor entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address (48 bits) of the static neighbor entry, in the format of H-H-H.

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number.

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

Usage guidelines

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

The device uniquely identifies a static neighbor entry by using the neighbor's IPv6 address and the number of the Layer 3 interface that connects to the neighbor. You can configure a static neighbor entry by using either of the following methods:

- **Method 1**—Associate a neighbor IPv6 address and link-layer address with the Layer 3 interface of the local node.
- **Method 2**—Associate a neighbor IPv6 address and link-layer address with a Layer 2 port in a VLAN containing the local node.

You can use either of the previous configuration methods to configure a static neighbor entry for a VLAN interface.

- If Method 1 is used, the neighbor entry is in INCMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry goes into REACH state.
- If Method 2 is used, the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id* and the corresponding VLAN interface must already exist. After the static neighbor entry is configured, the device associates the VLAN interface with the IPv6 address to uniquely identify the static neighbor entry. The entry will be in REACH state.

You can use the **undo ipv6 neighbor** command to delete both static and dynamic neighbor entries.

To delete a neighbor entry for a VLAN interface, specify only the corresponding VLAN interface.

Examples

Configure a static neighbor entry for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1
```

Related commands

display ipv6 neighbors

reset ipv6 neighbors

ipv6 neighbor link-local minimize

Use **ipv6 neighbor link-local minimize** to minimize link-local ND entries.

Use **undo ipv6 neighbor link-local minimize** to restore the default.

Syntax

ipv6 neighbor link-local minimize

undo ipv6 neighbor link-local minimize

Default

All ND entries are assigned to the driver.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Perform this command to minimize link-local ND entries assigned to the driver. Link-local ND entries refer to ND entries that contain link-local addresses.

With this feature enabled, the device does not add newly learned link-local ND entries whose link local addresses are not the next hop of any route to the driver. This saves driver resources.

This feature affects only newly learned link-local ND entries rather than existing ND entries.

Examples

Minimize link-local ND entries.

```
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

ipv6 neighbor stale-aging

Use **ipv6 neighbor stale-aging** to set the aging timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

Default

The aging timer for ND entries in stale state is 240 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state, in the range of 1 to 1440 minutes.

Usage guidelines

This aging time applies to all ND entries in stale state. If an ND entry in stale state is not updated before the timer expires, it moves to the delay state. If it is still not updated in 5 seconds, the ND entry moves to the probe state. The device sends an NS message for detection a maximum of three times. If no response is received, the device deletes the ND entry.

Examples

Set the aging timer for ND entries in stale state to 120 minutes.

```
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 120
```

ipv6 neighbors max-learning-num

Use **ipv6 neighbors max-learning-num** to set the maximum number of dynamic neighbor entries that an interface can learn. This prevents the interface from occupying too many neighbor table resources.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

Default

Hardware series	Model	Product code	Default
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	An interface can learn a maximum of 512 dynamic neighbor entries.
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	• WX2508H-PWR-LTE: An interface can learn a maximum of 2048 dynamic neighbor entries. • WX2510H-PWR, WX2510H-F-PWR: An interface can learn a maximum of 2048 dynamic neighbor entries. • WX2540H, WX2540H-F: An interface can learn a maximum of 3072 dynamic neighbor entries. • WX2560H: An interface can learn a maximum of 6144 dynamic neighbor entries.
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	6144
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR	• WX3010H, WX3010H-L-PWR, WX3024H-L-PWR: An interface can learn a

Hardware series	Model	Product code	Default
	WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	maximum of 4096 dynamic neighbor entries. • WX3010H-X-PWR: An interface can learn a maximum of 3072 dynamic neighbor entries. • WX3024H, WX3024H-F: An interface can learn a maximum of 8192 dynamic neighbor entries.
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H EWP-WX3510H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H	• WX3508H: An interface can learn a maximum of 8192 dynamic neighbor entries. • WX3510H: An interface can learn a maximum of 16384 dynamic neighbor entries. • WX3520H, WX3520H-F: An interface can learn a maximum of 32768 dynamic neighbor entries. • WX3540H: An interface can learn a maximum of 40960 dynamic neighbor entries.
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	• WX5510E: An interface can learn a maximum of 20480 dynamic neighbor entries. • WX5540E: An interface can learn a maximum of 61440 dynamic neighbor entries.
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	• WX5540H: An interface can learn a maximum of 61440 dynamic neighbor entries. • WX5560H, WX5580H: An interface can learn a maximum of 81920 dynamic neighbor entries.
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT	An interface can learn a maximum of 61440 dynamic neighbor entries.

Hardware series	Model	Product code	Default
	LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	Default
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	• WX1804H-PWR: An interface can learn a maximum of 512 dynamic neighbor entries. • WX1810H-PWR, WX1820H, WX1840H: An interface can learn a maximum of 2048 dynamic neighbor entries.
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	• WX3820H: An interface can learn a maximum of 32768 dynamic neighbor entries. • WX3840H: An interface can learn a maximum of 40960 dynamic neighbor entries.
WX5800H series	WX5860H	EWP-WX5860H-GL	An interface can learn a maximum of 65536 dynamic neighbor entries.

Views

Layer 2/Layer 3 interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic neighbor entries that an interface can learn.

The following compatibility matrixes show the value ranges for the *max-number* argument:

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	1 to 512
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	WX2508H-PWR-LTE: 1 to 2048 WX2510H-PWR: 1 to 2048 WX2510H-F-PWR: 1 to 2048 WX2540H: 1 to 3072

Hardware series	Model	Product code	Value range
			WX2540H-F: 1 to 3072 WX2560H: 1 to 6144
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	6144
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	WX3010H: 1 to 4096 WX3010H-L-PWR: 1 to 4096 WX3010H-X-PWR: 1 to 3072 WX3024H: 1 to 8192 WX3024H-L-PWR: 1 to 4096 WX3024H-F: 1 to 8192
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-PWR EWP-WX3510H EWP-WX3510H-PWR EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-PWR	WX3508H: 1 to 8192 WX3510H: 1 to 16384 WX3520H: 1 to 32768 WX3520H-F: 1 to 32768 WX3540H: 1 to 40960
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	WX5510E: 1 to 20480 WX5540E: 1 to 61440
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	WX5540H: 1 to 61440 WX5560H: 1 to 81920 WX5580H: 1 to 81920
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	1 to 61440

Hardware series	Model	Product code	Value range
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	WX1804H-PWR: 1 to 512 WX1810H-PWR: 1 to 2048 WX1820H: 1 to 2048 WX1840H: 1 to 2560
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	WX3820H: 1 to 32768 WX3840H: 1 to 40960
WX5800H series	WX5860H	EWP-WX5860H-GL	1 to 65536

Usage guidelines

The device can dynamically acquire the link-layer address of a neighboring node through NS and NA messages and add it into the neighbor table.

When the number of dynamic neighbor entries reaches the threshold, the interface stops learning neighbor information.

Examples

Set the maximum number of dynamic neighbor entries that VLAN-interface 100 can learn to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Use **ipv6 pathmtu** to set a static Path MTU for an IPv6 address.

Use **undo ipv6 pathmtu** to delete the Path MTU configuration for an IPv6 address.

Syntax

ipv6 pathmtu *ipv6-address value*

undo ipv6 pathmtu *ipv6-address*

Default

No static Path MTU is set.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

value: Specifies the Path MTU of the specified IPv6 address, in the range of 1280 to 10240 bytes.

Usage guidelines

You can set a static Path MTU for a destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static Path MTU of the specified destination IPv6 address. If the packet size is larger than the smaller one of the two values, the host fragments the packet according to the smaller value.

Examples

Set a static Path MTU for an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

Related commands

display ipv6 pathmtu

reset ipv6 pathmtu

ipv6 pathmtu age

Use **ipv6 pathmtu age** to set the aging time for a dynamic Path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Default

The aging time for dynamic Path MTU is 10 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

age-time: Specifies the aging time for Path MTU in minutes, in the range of 10 to 100.

Usage guidelines

After the path MTU from a source host to a destination host is dynamically determined, the source host sends subsequent packets to the destination host based on this MTU. After the aging time expires, the following events occur:

- The dynamic Path MTU is removed.
- The source host determines a dynamic path MTU through the Path MTU mechanism again.

The aging time is invalid for a static Path MTU.

Examples

Set the aging time for a dynamic Path MTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

Related commands

display ipv6 pathmtu

ipv6 prefer temporary-address

Use **ipv6 prefer temporary-address** to enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Use **undo ipv6 prefer temporary-address** to disable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Syntax

ipv6 prefer temporary-address

undo ipv6 prefer temporary-address

Default

The system is disabled to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The temporary address feature enables the system to generate and preferentially use the temporary IPv6 address of the sending interface as the source address of a packet. If the temporary IPv6 address cannot be used because of a DAD conflict, the system uses the public IPv6 address.

Examples

Enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of the packet.

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 temporary-address

ipv6 prefix

Use **ipv6 prefix** to configure a static IPv6 prefix.

Use **undo ipv6 prefix** to delete a static IPv6 prefix.

Syntax

ipv6 prefix *prefix-number ipv6-prefix/prefix-length*

undo ipv6 prefix *prefix-number*

Default

No static IPv6 prefix is configured.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies a prefix ID in the range of 1 to 1024.

ipv6-prefix/prefix-length: Specifies a prefix and its length. The value range for the *prefix-length* argument is 1 to 128.

Usage guidelines

To modify an existing static prefix, execute the **undo ipv6 prefix** command to delete the existing static prefix, and then execute the **ipv6 prefix** command.

Dynamic IPv6 prefixes obtained from DHCPv6 servers cannot be manually removed or modified.

A static IPv6 prefix can have the same prefix ID with a dynamic IPv6 prefix, but the static one takes precedence over the dynamic one.

Examples

Create static IPv6 prefix 2001:0410::/32 with prefix ID 1.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 2001:0410::/32
```

Related commands

display ipv6 prefix

ipv6 reassemble local enable

Use **ipv6 reassemble local enable** to enable IPv6 local fragment reassembly.

Use **undo ipv6 reassemble local enable** to disable IPv6 local fragment reassembly.

Syntax

ipv6 reassemble local enable

undo ipv6 reassemble local enable

Default

IPv6 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this command on a multichassis IRF fabric to improve fragment reassembly efficiency. The command enables the subordinate to reassemble the IPv6 fragments of a packet if all the fragments arrive at it. If this feature is disabled, all IPv6 fragments are delivered to the master for reassembly. The command applies only to fragments destined for the same subordinate.

Examples

Enable IPv6 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ipv6 reassemble local enable
```

ipv6 redirects enable

Use **ipv6 redirects enable** to enable sending ICMPv6 redirect messages.

Use **undo ipv6 redirects enable** to disable sending ICMPv6 redirect messages.

Syntax

ipv6 redirects enable

undo ipv6 redirects enable

Default

Sending ICMPv6 redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The default gateway sends an ICMPv6 redirect message to the source of an IPv6 packet to inform the source of a better first hop.

Sending ICMPv6 redirect messages enables hosts that hold few routes to establish routing tables and find the best route. Because this feature adds host routes into the routing tables, host performance degrades when there are too many host routes. As a result, sending ICMPv6 redirect messages is disabled by default.

Examples

Enable sending ICMPv6 redirect messages.

```
<Sysname> system-view
[Sysname] ipv6 redirects enable
```

ipv6 temporary-address

Use **ipv6 temporary-address** to enable the temporary IPv6 address feature.

Use **undo ipv6 temporary-address** to restore the default.

Syntax

ipv6 temporary-address [*valid-lifetime preferred-lifetime*]

undo ipv6 temporary-address

Default

The system does not generate any temporary IPv6 address.

Views

System view

Predefined user roles

network-admin

Parameters

valid-lifetime: Specifies the valid lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default valid lifetime is 604800 seconds (7 days).

preferred-lifetime: Specifies the preferred lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default preferred lifetime is 86400 seconds (1 day).

Usage guidelines

You must enable stateless autoconfiguration before enabling the temporary address feature.

The valid lifetime for temporary IPv6 addresses must be greater than or equal to the preferred lifetime for temporary IPv6 addresses.

In stateless address autoconfiguration, an interface automatically generates an IPv6 global unicast address by using the address prefix in the received RA message and the interface ID. On an IEEE 802 interface (such as an Ethernet interface or a VLAN interface), the interface ID is generated based on the interface's MAC address and is globally unique. An attacker can exploit this rule to easily identify the sending device.

To fix the vulnerability, you can enable the temporary address feature. An IEEE 802 interface generates the following addresses:

- **Public IPv6 address**—Includes an address prefix in the RA message and a fixed interface ID generated based on the interface's MAC address.
- **Temporary IPv6 address**—Includes an address prefix in the RA message and a random interface ID generated through MD5.

When the valid lifetime of a temporary IPv6 address expires, the system deletes the address and generates a new one. This enables the system to send packets with different source addresses through the same interface. The preferred lifetime and valid lifetime for a temporary IPv6 address are determined as follows:

- The preferred lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The preferred lifetime of the address prefix in the RA message.
  - The preferred lifetime configured for temporary IPv6 addresses minus DESYNC_FACTOR (a random number in the range of 0 to 600 seconds).
- The valid lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The valid lifetime of the address prefix.
  - The valid lifetime configured for temporary IPv6 addresses.

Examples

Enable the system to generate a temporary IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 prefer temporary-address

ipv6 unreachables enable

Use **ipv6 unreachables enable** to enable sending ICMPv6 destination unreachable messages.

Use **undo ipv6 unreachables** to disable sending ICMPv6 destination unreachable messages.

Syntax

ipv6 unreachables enable

undo ipv6 unreachables enable

Default

Sending ICMPv6 destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the device fails to forward a received IPv6 packet because of a destination unreachable error, it performs the following operations:

- Drops the packet.
- Sends an ICMPv6 destination unreachable message to the source.

If the device is generating ICMPv6 destination unreachable messages incorrectly, disable sending ICMPv6 destination unreachable messages to prevent attack risks.

Examples

Enable sending ICMPv6 destination unreachable messages.

```
<Sysname> system-view
[Sysname] ipv6 unreachables enable
```

local-proxy-nd enable

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to disable local ND proxy.

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

Default

Local ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Examples

Enable local ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] local-proxy-nd enable
```

Related commands

proxy-nd enable

proxy-nd enable

Use **proxy-nd enable** to enable common ND proxy.

Use **undo proxy-nd enable** to disable common ND proxy.

Syntax

proxy-nd enable

undo proxy-nd enable

Default

Common ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Examples

Enable common ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] proxy-nd enable
```

Related commands

local-proxy-nd enable

reset ipv6 nd snooping

Use **reset ipv6 nd snooping** to clear ND snooping entries.

Syntax

reset ipv6 nd snooping [[**vlan** *vlan-id*] [**global** | **link-local**] | **vlan** *vlan-id ipv6-address*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-address: Clears ND snooping entries for the specified IPv6 address.

vlan *vlan-id*: Clears ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

global: Clears ND snooping entries for global unicast addresses.

link-local: Clears ND snooping entries for link-local addresses.

Usage guidelines

If no option is specified, this command clears all ND snooping entries.

Examples

Clear all ND snooping entries.

```
<Sysname> reset ipv6 nd snooping
```

reset ipv6 neighbors

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

Syntax

In standalone mode:

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

In IRF mode:

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears static and dynamic neighbor information for all interfaces.

dynamic: Clears dynamic neighbor information for all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information for the interface specified by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears dynamic neighbor information for all member devices. (In IRF mode.)

static: Clears static neighbor information for all interfaces.

Examples

Clear neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors all
This will delete all the entries. Continue? [Y/N]:Y
```

Clear dynamic neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

Clear all neighbor information for GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

Related commands

display ipv6 neighbors

ipv6 neighbor

reset ipv6 pathmtu

Use **reset ipv6 pathmtu** to clear the Path MTU information.

Syntax

reset ipv6 pathmtu { **all** | **dynamic** | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all Path MTUs.

dynamic: Clears all dynamic Path MTUs.

static: Clears all static Path MTUs.

Examples

Clear all Path MTUs.

```
<Sysname> reset ipv6 pathmtu all
```

Related commands

display ipv6 pathmtu

reset ipv6 statistics

Use **reset ipv6 statistics** to clear IPv6 and ICMPv6 packet statistics.

Syntax

In standalone mode:

reset ipv6 statistics

In IRF mode:

reset ipv6 statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 and ICMPv6 packet statistics for all member devices. (In IRF mode.)

Examples

Clear IPv6 and ICMPv6 packet statistics.

```
<Sysname> reset ipv6 statistics
```

Related commands

display ipv6 statistics

Contents

Policy-based routing commands 1

apply continue 2
apply default-next-hop 3
apply default-output-interface 4
apply ip-df 5
apply loadshare 5
apply next-hop 7
apply output-interface 7
apply precedence 8
display ip policy-based-route 9
display ip policy-based-route interface 10
display ip policy-based-route local 12
display ip policy-based-route setup 13
if-match acl 14
ip local policy-based-route 14
ip policy-based-route 15
policy-based-route 16
reset ip policy-based-route statistics 17
snmp-agent trap enable policy-based-route 17

Policy-based routing commands

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

The following compatibility matrixes show the support of hardware platforms for policy-based routing:

Hardware series	Model	Product code	Policy-based routing compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	Yes

Hardware series	Model	Product code	Policy-based routing compatibility
	EWPXM2WCMD0F EWPXM1MAC0F	EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	Policy-based routing compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

apply continue

Use **apply continue** to compare packets with the next policy node upon failure on the current node.

Use **undo apply continue** to restore the default.

Syntax

apply continue

undo apply continue

Default

PBR does not compare packets with the next policy node upon failure on the current node.

Views

Policy node view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when the match mode of the node is **permit**.

This command applies when either of the following conditions exist:

- None of the following clauses is configured for packet forwarding:
  - **apply next-hop**
  - **apply output-interface**
  - **apply default-next-hop**
  - **apply default-output-interface**
- A clause listed above is configured, but it has become invalid. Then, a routing table lookup also fails for the matching packet.

NOTE:

A clause might become invalid because the specified next hop is unreachable or the specified output interface is down.

Examples

Compare with the next policy node upon failure on the current node.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply continue
```

apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

apply default-next-hop { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-n>

undo apply default-next-hop [*ip-address*&<1-n>]

Default

No default next hops are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a default next hop.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n default next hops, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple default next hops for backup or load sharing in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes the default next hop.

Without any default next hop specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Set a directly-connected default next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 direct
```

Related commands

apply loadshare

apply default-output-interface

Use **apply default-output-interface** to set default output interfaces.

Use **undo apply default-output-interface** to remove default output interfaces.

Syntax

apply default-output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-n>

undo apply default-output-interface [{ *interface-type interface-number* }&<1-n>]

Default

No default output interfaces are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

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

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n interfaces, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple default output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The default output interface must be P2P type. Using a non-P2P default output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast and non-broadcast multi-access (NBMA) interfaces such as Ethernet and virtual-template interfaces. In NBMA networks, packets are sent in unicast.

With a default output interface specified, the **undo apply default-output-interface** command removes the default output interface.

Without any default output interface specified, the **undo apply default-output-interface** command removes all default output interfaces.

Examples

Specify VLAN-interface 2 as the default output interface for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface vlan-interface 2
```

Related commands

apply loadshare

apply ip-df

Use **apply ip-df** to set the Don't Fragment (DF) bit in the IP header of matching packets.

Use **undo apply ip-df** to restore the default.

Syntax

apply ip-df *df-value*

undo apply ip-df

Default

The DF bit is not set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

df-value: Sets the DF bit in the IP header of matching packets. The value can be 0 or 1.

Usage guidelines

Setting the DF bit to 0 allows packet fragmentation.

Setting the DF bit to 1 prohibits packet fragmentation.

Examples

Set the DF bit in the IP header of matching packets to 0.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply ip-df 0
```

apply loadshare

Use **apply loadshare** to enable load sharing among multiple next hops, output interfaces, default next hops, or default output interfaces.

Use **undo apply loadshare** to restore the default.

Syntax

apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

undo apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

Default

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in primary/backup mode.

Views

Policy node view

Predefined user roles

network-admin

Parameters

default-next-hop: Enables load sharing among multiple default next hops.

default-output-interface: Enables load sharing among multiple default output interfaces.

next-hop: Enables load sharing among multiple next hops.

output-interface: Enables load sharing among multiple output interfaces.

Usage guidelines

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in either primary/backup or load sharing mode. For example:

- **Primary/backup mode**—The first configured output interface is used. When the primary output interface fails, the first configured backup output interface takes over.
- **Load sharing mode**—Multiple output interfaces load share traffic on a per-packet basis in turn, according to the configuration order.

NOTE:

Multiple next hops load share traffic according to their weights. By default, all next hops have the same weight and traffic is load balanced among them.

Examples

Enable load sharing among multiple next hops.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare next-hop
```

Enable load sharing among multiple output interfaces.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface vlan-interface 1 vlan-interface 2
[Sysname-pbr-aa-11] apply loadshare output-interface
```

Enable load sharing among multiple default next hops.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare default-next-hop
```

Enable load sharing among multiple default output interfaces.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface vlan-interface 1 vlan-interface 2
[Sysname-pbr-aa-11] apply loadshare default-output-interface
```

Related commands

apply default-next-hop

apply default-output-interface

apply next-hop

apply output-interface

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop { *ip-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] }&<1-n>

undo apply next-hop [*ip-address*&<1-n>]

Default

No next hops are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a next hop.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

weight *weight-value*: Specifies a load sharing weight for the next hop, in the range of 1 to 100. The default is 10. If you specify weights 1, 1, and 2 for three next hops, they share 1/4, 1/4, and 1/2 of the whole traffic, respectively.

&<1-n>: Indicates that you can specify up to n next hops, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple next hops for backup or load sharing in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

Related commands

apply loadshare

apply output-interface

Use **apply output-interface** to set output interfaces.

Use **undo apply output-interface** to remove output interfaces.

Syntax

apply output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-n>

undo apply output-interface [{ *interface-type interface-number* }&<1-n>]

Default

No output interfaces are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

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

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n interfaces, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The output interface must be P2P type. Using a non-P2P output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast and NBMA interfaces such as Ethernet and virtual-template interfaces.

With an output interface specified, the **undo apply output-interface** command removes the output interface.

Without any output interface specified, the **undo apply output-interface** command removes all output interfaces.

Examples

Specify VLAN-interface 2 as the output interface for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface vlan-interface 2
```

Related commands

apply loadshare

apply precedence

Use **apply precedence** to set a precedence for IP packets.

Use **undo apply precedence** to restore the default.

Syntax

apply precedence { *type* | *value* }

undo apply precedence

Default

No precedence is set for IP packets.

Views

Policy node view

Predefined user roles

network-admin

Parameters

type: Specifies the precedence type for IP packets.

value: Specifies the precedence for IP packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in Table 1. You can set either a precedence value or a precedence type for IP packets.

Table 1 IP precedences and corresponding types

Precedence value	Precedence type
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Examples

Set the precedence to 5 (critical) for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply precedence critical
```

display ip policy-based-route

Use **display ip policy-based-route** to display PBR policy information.

Syntax

display ip policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all PBR policies.

Examples

Display all policy information.

```
<Sysname> display ip policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

Table 2 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.

Related commands

policy-based-route

display ip policy-based-route interface

Use **display ip policy-based-route interface** to display interface PBR configuration and statistics.

Syntax

In standalone mode:

display ip policy-based-route interface *interface-type interface-number*

In IRF mode:

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device. (In IRF mode.)

Examples

Display PBR configuration and statistics on VLAN-interface 2.

```
<Sysname> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny(not support):
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
```

```
  node 2 permit(no resource):
    if-match acl 2000
    apply next-hop 2.2.2.2
    apply output-interface Vlan-interface3 track 1 (down)
    apply output-interface Vlan-interface4 track 2 (inactive)
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0 (no statistics resource)
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
apply output-interface track 1 (down)	Specifies an output interface and its associated track entry for permitted packets. This field displays the interface status in brackets. • **up**—The interface is up. • **down**—The interface is down at network layer. • **inactive**—The card that hosts the interface is not in position.

Field	Description
Matched	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

display ip policy-based-route local

Use **display ip policy-based-route local** to display local PBR configuration and statistics.

Syntax

In standalone mode:

display ip policy-based-route local

In IRF mode:

display ip policy-based-route local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays local PBR configuration and statistics for the master device. (In IRF mode.)

Examples

Display local PBR configuration and statistics.

```
<Sysname> display ip policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
```

```
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 4 Command output

Field	Description
Policy based routing information for local	Local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node: permit or deny.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

`reset ip policy-based-route statistics`

display ip policy-based-route setup

Use **`display ip policy-based-route setup`** to display PBR configuration.

Syntax

`display ip policy-based-route setup`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display PBR configuration.

```
<Sysname> display ip policy-based-route setup
Policy name             Type     Interface
pr01                    Forward  Vlan-interface2
aaa                     Local    N/A
```

Table 5 Command output

Field	Description
Policy name	Name of the PBR policy.

Field	Description
Type	PBR type: • **Forward**—Interface PBR. • **Local**—Local PBR.
Interface	Interface where the PBR policy is applied. This field displays **N/A** for local PBR.

Related commands

ip policy-based-route

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *acl-number* | **name** *acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for a basic ACL, and in the range of 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with letter *a* to *z* or *A* to *Z*. The ACL name cannot be **all**. For the command to take effect, make sure the specified ACL is a basic or advanced ACL.

Examples

Configure Node 11 of policy **aa** to permit the packets matching ACL 2011.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2011
```

Configure Node 11 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl name aaa
```

ip local policy-based-route

Use **ip local policy-based-route** to specify a policy for local PBR.

Use **undo ip local policy-based-route** to restore the default.

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

Default

No policy is specified for local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

Local PBR guides the forwarding of locally generated packets, such as ICMP packets generated by using the **ping** command.

Local PBR might affect local services, such as ping and Telnet. When you use local PBR, make sure you fully understand its impact on local services of the device.

You can specify only one policy for local PBR and must make sure the specified policy already exists.

Before you apply a new policy, you must first remove the current policy.

Examples

Configure local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

ip policy-based-route

Use **ip policy-based-route** to specify a policy for interface PBR on an interface.

Use **undo ip policy-based-route** to restore the default.

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

Default

No policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

policy-based-route

Use **policy-based-route** to create a policy node and enter its view, or enter the view of an existing policy node.

Use **undo policy-based-route** to delete a policy or policy node.

Syntax

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies a policy node by its number. A smaller number has a higher priority.

Usage guidelines

A policy that has been applied to an interface or locally cannot be deleted. To delete it, you must first cancel the application.

- If a policy node is specified, the **undo policy-based-route** command deletes the specified policy node.
- If a match mode is specified, the command deletes all nodes configured with the match mode.
- If no policy node or match mode is specified, the command deletes the whole policy.

Examples

Create permit-mode of Node 10 for policy **policy1** and enter its view.

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

```
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10]
```

Related commands

display ip policy-based-route

reset ip policy-based-route statistics

Use **reset ip policy-based-route statistics** to clear PBR statistics.

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears PBR statistics for all policies.

Examples

Clear all PBR statistics.

```
<Sysname> reset ip policy-based-route statistics
```

Related commands

display ip policy-based-route interface

display ip policy-based-route local

snmp-agent trap enable policy-based-route

Use **snmp-agent trap enable policy-based-route** to enable SNMP notifications for PBR.

Use **undo snmp-agent trap enable policy-based-route** to disable SNMP notifications for PBR.

Syntax

snmp-agent trap enable policy-based-route

undo snmp-agent trap enable policy-based-route

Default

SNMP notifications are enabled for PBR.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable this feature, PBR can generate notifications and send them to the SNMP module when the next hop becomes invalid. For the PBR notifications to be sent correctly, you must also

configure SNMP on the device. For more information about configuring SNMP, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for PBR.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable policy-based-route
```

Contents

IPv6 policy-based routing commands 1

apply continue 2
apply default-next-hop 3
apply default-output-interface 4
apply loadshare 5
apply next-hop 6
apply output-interface 7
apply precedence 8
display ipv6 policy-based-route 9
display ipv6 policy-based-route interface 9
display ipv6 policy-based-route local 11
display ipv6 policy-based-route setup 12
if-match acl 13
ipv6 local policy-based-route 14
ipv6 policy-based-route (interface view) 15
ipv6 policy-based-route (system view) 15
reset ipv6 policy-based-route statistics 16
snmp-agent trap enable ipv6 policy-based-route 17

IPv6 policy-based routing commands

The WX1800H series, WX2500H series, MAK series, and WA3000H series access controllers do not support parameters or commands that are available only in IRF mode.

The following compatibility matrixes show the support of hardware platforms for IPv6 policy-based routing:

Hardware series	Model	Product code	IPv6 policy-based routing compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT	Yes

Hardware series	Model	Product code	IPv6 policy-based routing compatibility
	EWPXM2WCMD0F EWPXM1MAC0F	EWPXM2WCMD0F EWPXM1MAC0F	

Hardware series	Model	Product code	IPv6 policy-based routing compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

apply continue

Use **apply continue** to compare packets with the next policy node upon failure on the current node.

Use **undo apply continue** to restore the default.

Syntax

apply continue

undo apply continue

Default

IPv6 PBR does not compare packets with the next policy node upon failure on the current node.

Views

IPv6 policy node view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when the mode of the node is **permit**.

This command applies when either of the following conditions exist:

- None of the following clauses is configured for packet forwarding:
  - **apply next-hop**
  - **apply output-interface**
  - **apply default-next-hop**
  - **apply default-output-interface**
- A clause listed above is configured, but it has become invalid. Then, a routing table lookup also fails for the matching packet.

NOTE:

A clause might become invalid because the specified next hop is unreachable or the specified output interface is down.

Examples

Compare with the next policy node upon failure on the current node.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply continue
```

apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

apply default-next-hop { *ipv6-address* [**direct**] [**track** *track-entry-number*] }&<1-n>

undo apply default-next-hop [*ipv6-address*&<1-n>]

Default

No default next hop is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a default next hop.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n default next hops, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple default next hops for backup or load sharing in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes the default next hop.

Without any default next hop specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Set a directly-connected default next hop of 1:1::1:1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1:1::1:1 direct
```

Related commands

apply loadshare

apply default-output-interface

Use **apply default-output-interface** to set default output interfaces.

Use **undo apply default-output-interface** to remove default output interfaces.

Syntax

apply default-output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-n>

undo apply default-output-interface [{ *interface-type interface-number* }&<1-n>]

Default

No default output interface is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

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

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n interfaces, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple default output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The default output interface must be P2P type. Using a non-P2P default output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast and non-broadcast multi-access (NBMA) interfaces such as Ethernet and virtual-template interfaces. In NBMA networks, packets are sent in unicast.

With a default output interface specified, the **undo apply default-output-interface** command removes the default output interface.

Without any default output interface specified, the **undo apply default-output-interface** command removes all default output interfaces.

Examples

Specify VLAN-interface 2 as the default output interface for IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-output-interface vlan-interface 2
```

Related commands

apply loadshare

apply loadshare

Use **apply loadshare** to enable load sharing among multiple next hops, output interfaces, default next hops, or default output interfaces.

Use **undo apply loadshare** to restore the default.

Syntax

apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

undo apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

Default

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in primary/backup mode.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

default-next-hop: Enables load sharing among multiple default next hops.

default-output-interface: Enables load sharing among multiple default output interfaces.

next-hop: Enables load sharing among multiple next hops.

output-interface: Enables load sharing among multiple output interfaces.

Usage guidelines

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in either primary/backup or load sharing mode. For example:

- **Primary/backup mode**—The first configured output interface is used. When the primary output interface fails, the first configured backup output interface takes over.
- **Load sharing mode**—Multiple output interfaces load share traffic on a per-packet basis in turn, according to the configuration order.

NOTE:

Multiple next hops load share traffic according to their weights. By default, all next hops have the same weight and traffic is load balanced among them.

Examples

Enable load sharing among multiple next hops.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1 2::2
[Sysname-pbr6-aa-11] apply loadshare next-hop
```

Enable load sharing among multiple output interfaces.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface vlan-interface 1 vlan-interface 2
```

```
[Sysname-pbr6-aa-11] apply loadshare output-interface
```

Enable load sharing among multiple default next hops.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1::1 2::2
[Sysname-pbr6-aa-11] apply loadshare default-next-hop
```

Enable load sharing among multiple default output interfaces.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-output-interface vlan-interface 1 vlan-interface 2
[Sysname-pbr6-aa-11] apply loadshare default-output-interface
```

Related commands

apply default-next-hop

apply default-output-interface

apply next-hop

apply output-interface

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop { *ipv6-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] } &<1-n>

undo apply next-hop [*ipv6-address*&<1-n>]

Default

No next hop is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a next hop.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

weight *weight-value*: Specifies a load sharing weight for the next hop, in the range of 1 to 100. The default is 10. If you specify weights 1, 1, and 2 for three next hops, they share 1/4, 1/4, and 1/2 of the whole traffic, respectively.

&<1-n>: Indicates that you can specify up to n next hops, each of which can be associated with a track entry. The value for n is 4.

Usage guidelines

You can specify multiple next hops for backup or load sharing in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1::1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1
```

Related commands

apply loadshare

apply output-interface

Use **apply output-interface** to set output interfaces.

Use **undo apply output-interface** to remove output interfaces.

Syntax

apply output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-n>

undo apply output-interface [{ *interface-type interface-number* }&<1-n>]

Default

No output interface is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

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

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-n>: Indicates that you can specify up to n interfaces, each of which can be associated with a track entry. The value for n varies by device model.

Usage guidelines

You can specify multiple output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The output interface must be P2P type. Using a non-P2P output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast and NBMA interfaces such as Ethernet and virtual-template interfaces.

With an output interface specified, the **undo apply output-interface** command removes the output interface.

Without any output interface specified, the **undo apply output-interface** command removes all output interfaces.

Examples

Specify VLAN-interface 2 as the output interface for IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface vlan-interface 2
```

Related commands

apply loadshare

apply precedence

Use **apply precedence** to set a precedence for IPv6 packets.

Use **undo apply precedence** to restore the default.

Syntax

apply precedence { *type* | *value* }

undo apply precedence

Default

No precedence is set for IPv6 packets.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

type: Specifies the precedence type for IPv6 packets.

value: Specifies the precedence for IPv6 packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in Table 1. You can set either a precedence value or a precedence type for IPv6 packets.

Table 1 IP precedences and the corresponding types

Precedence value	Precedence type
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Examples

Set the precedence to 5 (critical) for IPv6 packets.

```
<Sysname> system-view
[Sysname]ipv6 policy-based-route aa permit node 11
```

```
[Sysname-pbr6-aa-11] apply precedence critical
```

display ipv6 policy-based-route

Use **display ipv6 policy-based-route** to display IPv6 PBR policy information.

Syntax

display ipv6 policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all IPv6 PBR policies.

Examples

Display all IPv6 policy information.

```
<Sysname> display ipv6 policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

Table 2 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares IPv6 packets with IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.

Related commands

ipv6 policy-based-route (system view)

display ipv6 policy-based-route interface

Use **display ipv6 policy-based-route interface** to display IPv6 interface PBR configuration and statistics.

Syntax

In standalone mode:

display ipv6 policy-based-route interface *interface-type interface-number*

In IRF mode:

display ipv6 policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 interface PBR configuration and statistics for the master device. (In IRF mode.)

Examples

Display IPv6 PBR configuration and statistics on VLAN-interface 2.

```
<Sysname> display ipv6 policy-based-route interface Vlan-inerface2
Policy based routing information for interface Vlan-inerface2:
Policy name: aaa
  node 0 deny(not support):
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit(no resource):
    if-match acl 2000
    apply next-hop 1000::1
    apply output-interface Vlan-inerface3 track 1 (down)
    apply output-interface Vlan-inerface4 track 2 (inactive)
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0 (no statistics resource)
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	IPv6 PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.

Field	Description
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares IPv6 packets with the IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.
apply output-interface track 1 (down)	Specifies an output interface for permitted packets. The interface status includes the following: • **up**—The interface is up. • **down**—The interface is down at network layer. • **inactive**—The interface is not in position.
Matched	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

`reset ipv6 policy-based-route statistics`

display ipv6 policy-based-route local

Use **`display ipv6 policy-based-route local`** to display IPv6 local PBR configuration and statistics.

Syntax

In standalone mode:

`display ipv6 policy-based-route local`

In IRF mode:

`display ipv6 policy-based-route local` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 local PBR configuration and statistics for the master device. (In IRF mode.)

Examples

Display IPv6 local PBR configuration and statistics.

```
<Sysname> display ipv6 policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 2::2
  Matched: 0
Total matched: 0
```

Table 4 Command output

Field	Description
Policy based routing information for local	IPv6 local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node, **permit** or **deny**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ipv6 policy-based-route statistics

display ipv6 policy-based-route setup

Use **display ipv6 policy-based-route setup** to display IPv6 PBR configuration.

Syntax

display ipv6 policy-based-route setup

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 PBR configuration.

```
<Sysname> display ipv6 policy-based-route setup
Policy name             Type               Interface
pr01                    Forward            Vlan-interface 2
pr02                    Local              N/A
```

Table 5 Command output

Field	Description
Policy name	Name of the IPv6 PBR policy.
Type	IPv6 PBR type: • **Forward**—IPv6 interface PBR. • **Local**—IPv6 local PBR.
Interface	Interface where the IPv6 PBR policy is applied. This field displays **N/A** for IPv6 local PBR.

Related commands

ipv6 policy-based-route (interface view)

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999. The value range of a basic ACL is 2000 to 2999 and that of an advanced ACL is 3000 to 3999.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters starting with a letter. The ACL name cannot be **all**. For the command to take effect, make sure the specified IPv6 ACL is a basic or advanced ACL.

Examples

Configure Node 10 of policy **aa** to permit the packets matching ACL 2000.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl 2000
```

Configure Node 10 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl name aaa
```

ipv6 local policy-based-route

Use **ipv6 local policy-based-route** to configure IPv6 local PBR based on a specified policy.

Use **undo ipv6 local policy-based-route** to restore the default.

Syntax

ipv6 local policy-based-route *policy-name*

undo ipv6 local policy-based-route

Default

No policy is specified for IPv6 local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified IPv6 policy must already exist.

Usage guidelines

You can apply only one policy locally. Before you apply a new policy, you must first remove the current policy.

IPv6 local PBR is used to route locally generated packets except the packets destined for the sender. This feature might affect local services. Do not configure IPv6 local PBR unless doing so is required.

Examples

Configure IPv6 local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 local policy-based-route aaa
```

Related commands

display ipv6 policy-based-route setup

ipv6 policy-based-route (system view)

ipv6 policy-based-route (interface view)

Use **ipv6 policy-based-route** to configure IPv6 interface PBR by applying an IPv6 policy to an interface.

Use **undo ipv6 policy-based-route** to restore the default.

Syntax

ipv6 policy-based-route *policy-name*

undo ipv6 policy-based-route

Default

No IPv6 is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 policy-based-route aaa
```

Related commands

display ipv6 policy-based-route setup

ipv6 policy-based-route (system view)

ipv6 policy-based-route (system view)

Use **ipv6 policy-based-route** to create an IPv6 policy node and enter its view, or enter the view of an existing IPv6 policy node.

Use **undo ipv6 policy-based-route** to delete an IPv6 policy or IPv6 policy node.

Syntax

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No IPv6 policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies the number of the IPv6 policy node. A smaller number has a higher priority.

Usage guidelines

To delete an IPv6 policy that has already applied to an interface, you must delete the policy from the interface first.

If a policy node is specified, the **undo ipv6 policy-based-route** command deletes the specified policy node. If a match mode is specified, the command deletes all nodes configured with the match mode. If no node is specified, the command deletes the whole policy.

Examples

Create permit-mode Node 10 for IPv6 policy **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10]
```

Related commands

display ipv6 policy-based-route

reset ipv6 policy-based-route statistics

Use **reset ipv6 policy-based-route statistics** to clear IPv6 PBR statistics.

Syntax

reset ipv6 policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears IPv6 PBR statistics for all policies.

Examples

Clear all IPv6 PBR statistics.

```
<Sysname> reset ipv6 policy-based-route statistics
```

Related commands

display ipv6 policy-based-route interface

display ipv6 policy-based-route local

snmp-agent trap enable ipv6 policy-based-route

Use **snmp-agent trap enable ipv6 policy-based-route** to enable SNMP notifications for IPv6 PBR.

Use **undo snmp-agent trap enable ipv6 policy-based-route** to disable SNMP notifications for IPv6 PBR.

Syntax

snmp-agent trap enable ipv6 policy-based-route

undo snmp-agent trap enable ipv6 policy-based-route

Default

SNMP notifications are enabled for IPv6 PBR.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable this feature, IPv6 PBR can generate notifications and send them to the SNMP module when the next hop becomes invalid. For the IPv6 PBR notifications to be sent correctly, you must also configure SNMP on the device. For more information about configuring SNMP, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for IPv6 PBR.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ipv6 policy-based-route
```

Contents

GRE commands 1

gre checksum 1
gre key 1
keepalive 2

GRE commands

gre checksum

Use **gre checksum** to enable GRE checksum.

Use **undo gre checksum** to disable GRE checksum.

Syntax

gre checksum

undo gre checksum

Default

GRE checksum is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

GRE checksum verifies packet integrity.

You can enable or disable GRE checksum at each end of a tunnel as needed. After GRE checksum is enabled, the sender does the following:

- Calculates the checksum for the GRE header and the payload.
- Sends the packet containing the checksum information to the peer.

The receiver calculates the checksum for the received packet and compares it with that carried in the packet. If the checksums are the same, the receiver processes the packet. If the checksums are different, the receiver discards the packet.

If a packet carries a GRE checksum, the receiver checks the checksum whether or not the receiver is enabled with GRE checksum.

Examples

Enable GRE checksum.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] gre checksum
```

gre key

Use **gre key** to configure a key for a GRE tunnel interface.

Use **undo gre key** to restore the default.

Syntax

gre key *key*

undo gre key

Default

No key is configured for a GRE tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

key: Specifies the key for the GRE tunnel interface, in the range of 0 to 4294967295.

Usage guidelines

Both ends of a GRE tunnel must have the same key or no key.

Examples

Configure the GRE key as 123 for the GRE tunnel interface Tunnel 2.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] gre key 123
```

keepalive

Use **keepalive** to enable GRE keepalive and set the keepalive interval and the keepalive number.

Use **undo keepalive** to disable GRE keepalive.

Syntax

keepalive [*interval* [*times*]]

undo keepalive

Default

GRE keepalive is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the keepalive interval, in the range of 1 to 32767 seconds. The default value is 10.

times: Specifies the keepalive number, in the range of 1 to 255. The default value is 3.

Usage guidelines

This command enables the tunnel interface to send keepalive packets at the specified interval. If the device receives no response from the peer within the timeout time, it shuts down the local tunnel interface. The device brings the local tunnel interface up if it receives a keepalive acknowledgment packet from the peer. The timeout time is the result of multiplying the keepalive interval by the keepalive number.

The device always acknowledges the keepalive packets it receives whether or not GRE keepalive is enabled.

GRE/IPv6 mode tunnel interfaces do not support this command.

Examples

Enable GRE keepalive, set the keepalive interval to 20 seconds, and set the keepalive number to 5.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] keepalive 20 5
```

Contents

Tunneling commands ····· 1

bandwidth ····· 1
default ····· 1
description ····· 2
destination ····· 2
display interface tunnel ····· 3
interface tunnel ····· 7
mtu ····· 7
reset counters interface tunnel ····· 8
shutdown ····· 9
source ····· 9
tunnel dfbit enable ····· 10
tunnel out-interface ····· 11
tunnel tos ····· 12
tunnel ttl ····· 12

Tunneling commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface maximum rate divided by 1000.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth, in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth for an interface affects the link costs.

Examples

Set the expected bandwidth for Tunnel 1 to 100 kbps.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] bandwidth 100
```

default

Use **default** to restore the default settings for a tunnel interface.

Syntax

default

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands. Use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] default
```

description

Use **description** to configure the description of an interface.

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

Syntax

description *text*

undo description

Default

The description of a tunnel interface is **Tunnel***number* **Interface**, for example, **Tunnel1 Interface**.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure descriptions for different interfaces for identification and management purposes.

You can use the **display interface** command to display the configured interface description.

Examples

Configure the description of Tunnel 1 as **tunnel1**.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] description tunnel1
```

Related commands

display interface tunnel

destination

Use **destination** to specify the destination address for a tunnel interface.

Use **undo destination** to restore the default.

Syntax

destination { *ipv4-address* | *ipv6-address* }

undo destination

Default

No tunnel destination address is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the tunnel destination IPv4 address.

ipv6-address: Specifies the tunnel destination IPv6 address.

Usage guidelines

The tunnel destination address must be the address of the receiving interface on the tunnel peer. It is used as the destination address of tunneled packets.

The destination address of the local tunnel interface must be the source address of the peer tunnel interface. The source address of the local tunnel interface must be the destination address of the peer tunnel interface.

Do not specify the same tunnel source and destination addresses for the tunnel interfaces on the same device.

Examples

VLAN-interface 100 on Sysname 1 uses the IP address 193.101.1.1 and VLAN-interface 100 on Sysname 2 uses the IP address 192.100.1.1. Configure the source address 193.101.1.1 and destination address 192.100.1.1 for the tunnel interface on Sysname 1.

```
<Sysname1> system-view
[Sysname1] interface tunnel 1 mode gre
[Sysname1-Tunnel1] source 193.101.1.1
[Sysname1-Tunnel1] destination 192.100.1.1
```

Configure the source address 192.100.1.1 and destination address 193.101.1.1 for the tunnel interface on Sysname 2.

```
<Sysname2> system-view
[Sysname2] interface tunnel 1 mode gre
[Sysname2-Tunnel1] source 192.100.1.1
[Sysname2-Tunnel1] destination 193.101.1.1
```

Related commands

display interface tunnel

interface tunnel

source

display interface tunnel

Use **display interface tunnel** to display tunnel interface information.

Syntax

display interface [**tunnel** [*number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. The specified tunnel interface must have been created. If you do not specify the **tunnel** keyword, this command displays information about all interfaces on the device. If you specify the **tunnel** keyword without the *number* argument, this command displays information about all existing tunnel interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in the physical state of DOWN and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed information about Tunnel 1.

```
<Sysname> display interface tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1476
Internet address: 10.1.2.1/24 (primary)
Tunnel source 2002::1:1 (Vlan-interface10), destination 2001::2:1
Tunnel TOS 0xC8, Tunnel TTL 255
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 1 Command output

Field	Description
Tunnel1	Information about the tunnel interface Tunnel 1.
Current state	Physical link state of the tunnel interface: • **Administratively DOWN**—The interface has been shut down

Field	Description
	by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description of the tunnel interface.
Bandwidth	Expected bandwidth of the tunnel interface.
Maximum transmission unit	MTU of the tunnel interface.
Internet protocol processing: Disabled	The tunnel interface is not assigned an IP address and cannot process IP packets.
Internet address	IP address of the tunnel interface. The **primary** attribute indicates that the address is the primary IP address.
Tunnel source	Source address of the tunnel. If a source interface is specified for the tunnel interface, this field also displays the source interface in parentheses.
destination	Destination address of the tunnel.
Tunnel keepalive enabled, Period(50 s), Retries(3)	Keepalive is enabled for GRE. In this example, the keepalive interval is 50 seconds and the keepalive number is 3.
Tunnel TOS	ToS of tunneled packets.
Tunnel TTL	TTL of tunneled packets.
Tunnel protocol/transport	Tunnel mode and transport protocol: • **GRE/IP**—GRE/IPv4 tunnel mode. • **GRE/IPv6**—GRE/IPv6 tunnel mode.
GRE key disabled	No GRE tunnel interface key is configured.
Checksumming of GRE packets disabled	The GRE packet checksum feature is disabled.
Last clearing of counters	Last time when counters were cleared.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate in the last 300 seconds.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate in the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Total input packets, total input bytes, and total input packets dropped.
Output: 0 packets, 0 bytes, 0 drops	Total output packets, total output bytes, and total output packets dropped.

Display brief information about Tunnel 1.

```
<Sysname> display interface tunnel 1 brief
```

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP   UP       1.1.1.1        Tunnel1
```

Display brief information about Tunnel 1, including the complete interface description.

```
<Sysname> display interface tunnel 1 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP    UP      1.1.1.1        Tunnel1
```

Display information about interfaces in DOWN state and the causes.

```
<Sysname> display interface tunnel brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Tun0                  DOWN Not connected
Tun1                  DOWN Not connected
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—The tunnel is not established.

Related commands

destination

interface tunnel

source

interface tunnel

Use **interface tunnel** to create a tunnel interface, specify the tunnel mode, and enter tunnel interface view, or enter the view of an existing tunnel interface.

Use **undo interface tunnel** to delete a tunnel interface.

Syntax

interface tunnel *number* [**mode gre** [**ipv6**]]

undo interface tunnel *number*

Default

No tunnel interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the number of the tunnel interface. The value range is 0 to 1023. The number of tunnel interfaces that can be created is restricted by the total number of interfaces and the memory.

mode gre: Specifies the GRE/IPv4 tunnel mode.

mode gre ipv6: Specifies the GRE/IPv6 tunnel mode.

Usage guidelines

To create a new tunnel interface, you must specify the tunnel mode in this command. To enter the view of an existing tunnel interface, you do not need to specify the tunnel mode.

A tunnel interface number is locally significant. The tunnel interfaces on the two ends of a tunnel can use the same or different interface numbers.

Examples

Create GRE/IPv4 tunnel interface Tunnel 1 and enter tunnel interface view.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1]
```

Related commands

destination

display interface tunnel

source

mtu

Use **mtu** to set the MTU on a tunnel interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

If the tunnel interface has never been up, the MTU is 64000 bytes.

If the tunnel interface is up, its MTU is identical to the outgoing interface's MTU minus the length of the tunnel headers. The outgoing interface is automatically obtained through routing table lookup based on the tunnel destination address.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU, in the range of 100 to 64000 bytes.

Usage guidelines

After you configure an MTU for a tunnel interface, the configured MTU applies regardless of the tunnel interface status (up/down) and the outgoing interface MTU.

To avoid fragmentation after tunnel encapsulation, set the tunnel interface MTU no greater than the value of the outgoing interface MTU minus the length of the tunnel headers.

Examples

Set the MTU on Tunnel 1 to 1000 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] mtu 1000
```

Related commands

display interface tunnel

reset counters interface tunnel

Use **reset counters interface tunnel** to clear tunnel interface statistics.

Syntax

reset counters interface [**tunnel** [*number*]]

Views

User view

Predefined user roles

network-admin

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. If you do not specify the **tunnel** keyword, this command clears statistics for all interfaces. If you specify the **tunnel** keyword without the *number* argument, this command clears statistics for all tunnel interfaces.

Usage guidelines

Use this command to clear old statistics so you can observe new traffic statistics on a tunnel interface.

Examples

Clear statistics for Tunnel 1.

```
<Sysname> reset counters interface tunnel 1
```

Related commands

display interface tunnel

shutdown

Use **shutdown** to shut down a tunnel interface.

Use **undo shutdown** to bring up a tunnel interface.

Syntax

shutdown

undo shutdown

Default

A tunnel interface is not administratively down.

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

This command disconnects all links set up on the interface. Make sure you fully understand the impact of the command on your network.

Examples

Shut down Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] shutdown
```

Related commands

display interface tunnel

source

Use **source** to specify the source address or source interface for a tunnel interface.

Use **undo source** to restore the default.

Syntax

source { *ipv4-address* | *ipv6-address* | *interface-type interface-number* }

undo source

Default

No source address or source interface is specified for a tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the tunnel source IPv4 address.

ipv6-address: Specifies the tunnel source IPv6 address.

interface-type interface-number: Specifies the source interface by its type and number. The interface must be up and must have an IP address.

Usage guidelines

The specified source address or the address of the specified source interface is used as the source address of tunneled packets. To display the configured tunnel source address, use the **display interface tunnel** command.

Do not specify the same tunnel source and destination addresses for the tunnel interfaces on the same device.

The destination address of the local tunnel interface must be the source address of the peer tunnel interface. The source address of the local tunnel interface must be the destination address of the peer tunnel interface.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify VLAN-interface 10 as the source interface of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source vlan-interface 10
```

Specify 192.100.1.1 as the source address of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source 192.100.1.1
```

Related commands

destination

display interface tunnel

interface tunnel

tunnel dfbit enable

Use **tunnel dfbit enable** to set the Don't Fragment (DF) bit for tunneled packets.

Use **undo tunnel dfbit enable** to restore the default.

Syntax

tunnel dfbit enable

undo tunnel dfbit enable

Default

The DF bit is not set for tunneled packets.

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

To avoid fragmentation and delay, set the DF bit for tunneled packets. Make sure the path MTU is larger than the tunneled packet length. To avoid discarding tunneled packets whose length is larger than the path MTU, do not set the DF bit.

This command is not supported on a GRE/IPv6 tunnel interface.

Examples

Set the DF bit for tunneled packets on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] tunnel dfbit enable
```

tunnel out-interface

Use **tunnel out-interface** to specify an output interface for tunneled packets.

Use **undo tunnel out-interface** to restore the default.

Syntax

tunnel out-interface *interface-type interface-number*

undo tunnel out-interface

Default

No output interface is specified for tunneled packets of a tunnel interface. If ECMP routes exist, the device randomly selects an output interface to forward the tunneled packets.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

Use this command to control the forwarding path of tunneled packets. To ensure successful packet forwarding, the specified output interface must meet the following requirements:

- The interface is up.
- The interface has an IP address.
- The interface has a route to reach the destination.

If you execute this command multiple times, the most recent configuration takes effect.

This command is applicable only to IPv4 ADVPN, IPv6 ADVPN, GRE/IPv4, GRE/IPv6, and VXLAN tunnel interfaces.

This command takes effect only on tunneled packets that are processed by CPUs. Whether the CPUs process tunneled packets depends on the device model.

Examples

Specify VLAN-interface 1 as the output interface of GRE packets on tunnel interface **Tunnel 0**.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre
[Sysname-Tunnel0] tunnel out-interface vlan-interface 1
```

tunnel tos

Use **tunnel tos** to set the ToS of tunneled packets.

Use **undo tunnel tos** to restore the default.

Syntax

tunnel tos *tos-value*

undo tunnel tos

Default

The ToS of tunneled packets is the same as that of the original packets.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

tos-value: Specifies the ToS of tunneled packets, in the range of 0 to 255.

Usage guidelines

After you execute this command, all the tunneled packets of different services sent on the tunnel interface will use the same configured ToS. For more information about ToS, see *QoS Configuration Guide*.

Examples

Set the ToS of tunneled packets to 20 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] tunnel tos 20
```

Related commands

display interface tunnel

tunnel ttl

Use **tunnel ttl** to set the Time to Live (TTL) of tunneled packets.

Use **undo tunnel ttl** to restore the default.

Syntax

tunnel ttl *ttl-value*

undo tunnel ttl

Default

The TTL of tunneled packets is 255.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ttl-value: Specifies the TTL of tunneled packets, in the range of 1 to 255.

Usage guidelines

The TTL determines the maximum number of hops that the tunneled packets can pass. When the TTL expires, the tunneled packets are discarded to avoid loops.

Examples

Set the TTL of tunneled packets to 100 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] tunnel ttl 100
```

Related commands

display interface tunnel

Contents

Basic IP routing commands 1

address-family ipv4 1
address-family ipv6 1
display ip routing-table 2
display ip routing-table acl 6
display ip routing-table *ip-address* 8
display ip routing-table prefix-list 11
display ip routing-table protocol 13
display ip routing-table statistics 14
display ip routing-table summary 15
display ipv6 rib graceful-restart 16
display ipv6 rib nib 16
display ipv6 route-direct nib 18
display ipv6 routing-table 20
display ipv6 routing-table acl 23
display ipv6 routing-table *ipv6-address* 27
display ipv6 routing-table prefix-list 30
display ipv6 routing-table protocol 31
display ipv6 routing-table statistics 33
display ipv6 routing-table summary 34
display max-ecmp-num 34
display rib graceful-restart 36
display rib nib 37
display route-direct nib 41
fib lifetime 44
inter-protocol fast-reroute 44
max-ecmp-num 45
non-stop-routing 47
protocol lifetime 49
reset ip routing-table statistics protocol 49
reset ipv6 routing-table statistics protocol 50
rib 50

Basic IP routing commands

address-family ipv4

Use **address-family ipv4** to create the RIB IPv4 address family and enter its view, or enter the view of the existing RIB IPv4 address family.

Use **undo address-family ipv4** to delete the RIB IPv4 address family and all settings in the view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No RIB IPv4 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv4 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4]
```

address-family ipv6

Use **address-family ipv6** to create the RIB IPv6 address family and enter its view, or enter the view of the existing RIB IPv6 address family.

Use **undo address-family ipv6** to delete the RIB IPv6 address family and all settings in the view.

Syntax

address-family ipv6

undo address-family ipv6

Default

No RIB IPv6 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv6 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv6
[Sysname-rib-ipv6]
```

display ip routing-table

Use **display ip routing-table** to display routing table information.

Syntax

display ip routing-table [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays routing table information for the public network.

Examples

Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table

Destinations : 12        Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

```
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0           192.168.1.40    Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

Table 1 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address/mask length.
Proto	Protocol that installed the route.
Pre	Preference of the route.
Cost	Cost of the route.
NextHop	Next hop address of the route.
Interface	Output interface for packets to be forwarded along the route.
Summary count	Number of routes.

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose

Destinations : 2        Routes : 2

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h34m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x10000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1000c       OrigNextHop: 127.0.0.1
      Label: NULL          RealNextHop: 127.0.0.1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A
```

```
Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 60
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.47.4
      Label: NULL           RealNextHop: 192.168.47.4
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A               VpnPeerId: N/A
       Dscp: N/A
```

Table 2 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	Destination address/mask length.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Route tag.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. This state is not supported in the current software version. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.

Field	Description
OrigVrf	This field is not supported in the current software version. Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	This field is not supported in the current software version. Original AS number.
NibID	ID of the next hop.
LastAs	This field is not supported in the current software version. Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
Label	This field is not supported in the current software version. Label.
RealNextHop	Real next hop of the route.
BkLabel	This field is not supported in the current software version. Backup label.
BkNexthop	Backup next hop.
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	This field is not supported in the current software version. BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if the BGP connector attribute is not supported.
VpnPeerId	This field is not supported in the current software version. ID of the VPN peer to which the route belongs, in the range of 1 to 134217727. This field displays **N/A** when the value is invalid.
Dscp	DSCP value of the route, in the range of 0 to 63. This field displays **N/A** when the value is invalid.
Summary count	Number of routes.

display ip routing-table acl

Use **display ip routing-table acl** to display information about routes permitted by a basic ACL.

Syntax

display ip routing-table acl *ipv4-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4-acl-number: Specifies a basic ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, the command displays information about all routes.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-ipv4-basic-2000] display ip routing-table acl 2000

Summary count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.1.0/24      Direct 0    0            192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0            192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0            192.168.1.111   Vlan11
```

For command output, see Table 1.

Display detailed information about all routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
```

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x10080       OrigNextHop: 192.168.1.111
      Label: NULL          RealNextHop: 192.168.1.111
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL          RealNextHop: 192.168.1.111
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A

Destination: 192.168.1.111/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
```

```
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x10004        OrigNextHop: 127.0.0.1
      Label: NULL           RealNextHop: 127.0.0.1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 2.

display ip routing-table *ip-address*

Use **display ip routing-table** *ip-address* to display information about routes to a specific destination address.

Use **display ip routing-table** *ip-address1* **to** *ip-address2* to display information about routes to a range of destination addresses.

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* **to** *ip-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies a destination IP address in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the IP address mask in dotted decimal notation.

longer-match: Displays the route entry with the longest mask.

ip-address1 **to** *ip-address2*: Specifies a destination IP address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different outputs.

- **display ip routing-table** *ip-address*
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ip routing-table** *ip-address mask*
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for an entry with a subnet mask not greater than the entered subnet mask, the entry is displayed.
- **display ip routing-table** *ip-address* **longer-match**
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for multiple entries, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address mask* **longer-match**

- The system ANDs the entered destination IP address with the entered subnet mask.
- The system ANDs the destination IP address in each active route entry with the entered subnet mask.

If the two operations yield the same result for multiple entries with a mask not greater than the entered subnet mask, the entry with the longest mask length is displayed.

- **display ip routing-table** *ip-address1* **to** *ip-address2*

  The system displays active route entries with destinations in the range of *ip-address1*/32 to *ip-address2*/32.

Examples

Display brief information about the routes to the destination IP address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1

Summary count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20

Summary count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
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
3.3.3.1/32          Direct 0    0            127.0.0.1       InLoop0
4.4.4.1/32          Direct 0    0            127.0.0.1       InLoop0
```

Display detailed information about the routes to the destination IP address 1.2.3.4.

```
<Sysname> display ip routing-table 1.2.3.4 verbose

Summary count : 1

Destination: 1.2.3.4/32
   Protocol: O_INTRA
 Process ID: 0
  SubProtID: 0x1                  Age: 00h00m37s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 200
      NibID: 0x15000000         LastAs: 200
     AttrID: 0x0              Neighbor: 192.168.47.2
      Flags: 0x10060       OrigNextHop: 192.168.47.2
      Label: NULL          RealNextHop: 192.168.47.2
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 2.

display ip routing-table prefix-list

Use **display ip routing-table prefix-list** to display routes permitted by an IP prefix list.

Syntax

display ip routing-table prefix-list *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all routes permitted by the IP prefix list. If you do not specify this keyword, the command displays brief information about active routes permitted by the IP prefix list.

Usage guidelines

If the specified IP prefix list does not exist, the command displays information about all routes.

Examples

Create an IP prefix list named **test** to permit the route 1.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip prefix-list test permit 1.1.1.0 24
```

Display brief information about the active route permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.0/24          Direct 0    0            1.1.1.2         Vlan11
```

For command output, see Table 1.

Display detailed information about all routes permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test verbose

Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 1.1.1.2
      Label: NULL           RealNextHop: 1.1.1.2
    BkLabel: NULL             BkNextHop: N/A
```

```
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 2.

display ip routing-table protocol

Use **display ip routing-table protocol** to display information about routes installed by a protocol.

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct

Summary count : 9

Direct Routing table status : <Active>
Summary count : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0            2.2.2.1         Vlan2
2.2.2.0/32          Direct 0    0            2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.255/32        Direct 0    0            2.2.2.1         Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  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

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
```

display ip routing-table statistics

Use **display ip routing-table statistics** to display IPv4 route statistics, including numbers of total routes, routes installed by the protocol, routes marked as deleted, and active routes.

Syntax

display ip routing-table statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If you do not specify any parameters, the command displays IPv4 route statistics for the public network.

Examples

Display IPv4 route statistics for the public network.

```
<Sysname> display ip routing-table statistics

Total prefixes: 15        Active prefixes: 15

Proto      route       active      added       deleted
DIRECT     12          12          30          18
STATIC     3           3           5           2
```

```
RIP        0           0           0           0
Total      15          15          35          20
```

Table 3 Command output

Field	Description
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ip routing-table summary

Use **display ip routing-table summary** to display brief routing table information, including maximum number of ECMP routes, maximum number of active routes, and number of remaining active routes.

Syntax

display ip routing-table summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief routing table information for the public network.

```
<Sysname> display ip routing-table summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262126
```

Table 4 Command output

Field	Description
Max ECMP	Maximum number of ECMP routes supported by the system.
Max Active Route	Maximum number of supported routes.
Remain Active Route	Number of the remaining inactive routes.

display ipv6 rib graceful-restart

Use **display ipv6 rib graceful-restart** to display IPv6 RIB GR state information.

Syntax

display ipv6 rib graceful-restart

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 RIB GR state information.

```
<Sysname> display ipv6 rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT6    480      29   End      No/No
 2    STATIC6    480      32   End      No/No
```

For command output, see Table 9.

display ipv6 rib nib

Use **display ipv6 rib nib** to display next hop information in the IPv6 RIB.

Syntax

display ipv6 rib nib [**self-originated**] [*nib-id*] [**verbose**]

display ipv6 rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

self-originated: Displays information about next hops of self-originated routes in the IPv6 RIB.

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information in the IPv6 RIB. If you do not specify this keyword, the command displays brief next hop information in the IPv6 RIB.

protocol *protocol*: Specifies a protocol by its name.

Examples

Display brief next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib
Total number of nexthop(s): 151

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid

...
```

Display detailed next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib verbose
Total number of nexthop(s): 151

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
```

```
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x26000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 121::2
    IFIndex: 0x112            LocalAddr: ::
   TopoNthp: Invalid
   Instance: default

      NibID: 0x26000002        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 122::2
    IFIndex: 0x112            LocalAddr: ::
   TopoNthp: Invalid
   Instance: abc

...
```

For command output, see Table 10 and Table 11.

display ipv6 route-direct nib

Use **display ipv6 route-direct nib** to display next hop information for IPv6 direct routes.

Syntax

display ipv6 route-direct nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information for IPv6 direct routes. If you do not specify this keyword, the command displays brief next hop information for IPv6 direct routes.

Examples

Display brief next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib
Total number of nexthop(s): 115

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid

...
```

Display detailed next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib verbose
Total number of nexthop(s): 115

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
```

```
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

For command output, see Table 12 and Table 13.

display ipv6 routing-table

Use **display ipv6 routing-table** to display IPv6 routing table information.

Syntax

display ipv6 routing-table [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays IPv6 routing table information for the public network.

Examples

Display brief information about active routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table

Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0
```

```
Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : InLoop0                                    Cost      : 0
```

Table 5 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	IPv6 address and prefix of the destination network or host.
NextHop	Next hop address of the route.
Preference	Preference of the route.
Interface	Output interface for packets to be forwarded along the route.
Protocol	Protocol that installed the route.
Cost	Cost of the route.
Summary count	Number of routes.

Display detailed information about all routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table verbose

Destinations : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h23m02s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa               OrigAs: 0
      NibID: 0x20000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
```

```
  SubProtID: 0x0                  Age: 00h01m47s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10080       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A
```

Table 6 Command output

Field	Description
Destination	IPv6 address and prefix of the destination network or host.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Tag of the route.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. This state is not supported in the current software version. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.
OrigVrf	This field is not supported in the current software version. Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	This field is not supported in the current software version. Original AS number.

Field	Description
NibID	ID of the next hop.
LastAs	This field is not supported in the current software version. Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
Label	This field is not supported in the current software version. Label.
RealNextHop	Real next hop of the route.
BkLabel	This field is not supported in the current software version. Backup label.
BkNexthop	Backup next hop.
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	This field is not supported in the current software version. BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if BGP connector attribute is not supported.
VpnPeerId	This field is not supported in the current software version. ID of the VPN peer to which the route belongs, in the range of 1 to 134217727. This field displays **N/A** when the value is invalid.
Dscp	DSCP value of the route, in the range of 0 to 63. This field displays **N/A** when the value is invalid.
Summary count	Number of routes.

display ipv6 routing-table acl

Use **display ipv6 routing-table acl** to display routing information permitted by an IPv6 basic ACL.

Syntax

display ipv6 routing-table acl *ipv6-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-acl-number: Specifies a basic IPv6 ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic IPv6 ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic IPv6 ACL.

Usage guidelines

If the specified IPv6 ACL does not exist or has no rules configured, the command displays information about all IPv6 routes.

Examples

Display brief information about active routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000

Summary count : 6

Destination : ::1/128                                 Protocol  : Direct
NextHop     : ::1                                     Preference: 0
Interface   : InLoop0                                 Cost      : 0

Destination: 12::/96                                  Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan11                                   Cost      : 0

Destination: 12::1/128                                Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 11::1/128                                Protocol  : O_INTER
NextHop    : FE80::A1F:3FFF:FE45:206                  Preference: 10
Interface  : Vlan11                                   Cost      : 2

Destination: FE80::/10                                Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: FF00::/8                                 Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0                                    Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000 verbose

Summary count : 6

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A               VpnPeerId: N/A
       Dscp: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 00h07m57s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000003         LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10080        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A               VpnPeerId: N/A
       Dscp: N/A

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
```

```
  SubProtID: 0x0                  Age: 00h07m55s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A

Destination: FE80::/10
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10084       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A

Destination: FF00::/8
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000001         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
```

```
      Flags: 0x10014        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: NULL0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 6.

display ipv6 routing-table *ipv6-address*

Use **display ipv6 routing-table** *ipv6-address* to display information about routes to an IPv6 destination address.

Use **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* to display information about routes to a range of IPv6 destination addresses.

Syntax

display ipv6 routing-table *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table *ipv6-address1* **to** *ipv6-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

longer-match: Displays the route entry with the longest prefix.

ipv6-address1 **to** *ipv6-address2*: Specifies a destination IPv6 address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different output.

- **display ipv6 routing-table** *ipv6-address*

- The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
- The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

If the two operations yield the same result for an entry, the entry is displayed.

- **display ipv6 routing-table** *ipv6-address prefix-length*
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for an entry with a prefix length not greater than the entered prefix length, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address* **longer-match**
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for multiple entries, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for multiple entries with a prefix length not greater than the entered prefix length, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2*

  The system displays route entries with destinations in the range of *ipv6-address1*/128 to *ipv6-address2*/128.

Examples

Display brief information about the routes to the destination IPv6 address 10::1 127.

```
<Sysname> display ipv6 routing-table 10::1 127

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 most specific route to the destination IPv6 address 10::1 and prefix length 127.

```
<Sysname> display ipv6 routing-table 10::1 127 longer-match

Summary count : 1

Destination: 10::/120                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display brief information about the routes to destination addresses in the range of 100:: to 300::.

```
<Sysname> display ipv6 routing-table 100:: to 300::

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
```

Display detailed information about the routes to destination IPv6 addresses 1:2::3:4/128.

```
<Sysname> display ipv6 routing-table 1:2::3:4 128 verbose

Summary count : 1

Destination: 1:2::3:4/128
   Protocol: Direct
 Process ID: 1
  SubProtID: 0x1                    Age: 00h01m14s
       Cost: 1               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x23000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10041        OrigNextHop: FE80::A1F:3FFF:FE45:206
      Label: NULL           RealNextHop: FE80::A1F:3FFF:FE45:206
```

```
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 6.

display ipv6 routing-table prefix-list

Use **display ipv6 routing-table prefix-list** to display information about IPv6 routes permitted by an IPv6 prefix list.

Syntax

display ipv6 routing-table prefix-list *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all IPv6 routes permitted by the IPv6 prefix list. If you do not specify this keyword, the command displays brief information about active IPv6 routes permitted by the IPv6 prefix list.

Usage guidelines

If the specified IPv6 prefix list does not exist, the command displays information about all routes.

Examples

Create an IPv6 prefix list named test to permit the prefix ::1/128.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list test permit ::1 128
```

Display brief information about the active IPv6 route permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test

Summary count : 1

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test verbose

Summary count : 1

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h57m19s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A
```

For command output, see Table 6.

display ipv6 routing-table protocol

Use **display ipv6 routing-table protocol** to display information about IPv6 routes installed by a protocol.

Syntax

display ipv6 routing-table protocol *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about IPv6 direct routes.

```
<Sysname> display ipv6 routing-table protocol direct

Summary count : 3

Direct Routing table status : <Active>
Summary count : 3

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Direct Routing table status : <Inactive>
Summary count : 0
```

Display brief information about IPv6 static routes.

```
<Sysname> display ipv6 routing-table protocol static

Summary count : 3

Static Routing table status : <Active>
Summary count : 3

Destination: 2::2/128                               Protocol  : Static
NextHop    : fe80::2                                Preference: 60
Interface  : Vlan12                                 Cost      : 0

Destination: 2::2/128                               Protocol  : Static
NextHop    : fe80::3                                Preference: 60
Interface  : Vlan12                                 Cost      : 0

Destination: 3::3/128                               Protocol  : Static
NextHop    : 2::2                                   Preference: 60
Interface  : Vlan12                                 Cost      : 0
```

```
Static Routing table status : <Inactive>
Summary count : 0
```

display ipv6 routing-table statistics

Use **display ipv6 routing-table statistics** to display IPv6 route statistics, including numbers of total routes, routes installed and deleted by the protocol, and active routes.

Syntax

display ipv6 routing-table statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If you do not specify any parameters, the command displays IPv6 route statistics for the public network.

Examples

Display IPv6 route statistics for the public network.

```
<Sysname> display ipv6 routing-table statistics

Total prefixes: 8        Active prefixes: 8

Proto      route       active      added       deleted
DIRECT     5           5           5           0
STATIC     3           3           3           0
RIPng      0           0           0           0
Total      8           8           8           0
```

Table 7 Command output

Field	Description
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ipv6 routing-table summary

Use **display ipv6 routing-table summary** to display brief IPv6 routing table information, including maximum number of ECMP routes, maximum number of active routes, and number of remaining active routes.

Syntax

display ipv6 routing-table summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief IPv6 routing table information for the public network.

```
<Sysname> display ipv6 routing-table summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262126
```

For command output, see Table 4.

display max-ecmp-num

Use **display max-ecmp-num** to display the maximum number of IPv4 ECMP routes.

Syntax

display max-ecmp-num

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes

Hardware series	Model	Product code	Command compatibility
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-L-PWR • WX3024H • WX3024H-L-PWR • WX3024H-F No: WX3010H-X-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of IPv4 ECMP routes.

```
<Sysname> display max-ecmp-num
  Max-ECMP-Num in use: 6
  Max-ECMP-Num at the next reboot: 10
```

Table 8 Command output

Field	Description
Max-ECMP-Num in use	Maximum number of current IPv4 ECMP routes in use.
Max-ECMP-Num at the next reboot	Maximum number of IPv4 ECMP routes at the next reboot of the device.

display rib graceful-restart

Use **`display rib graceful-restart`** to display RIB GR state information.

Syntax

`display rib graceful-restart`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display RIB GR state information.

```
<Sysname> display rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT     100      30   End      No/No
 2    STATIC     480      34   End      No/No
```

Table 9 Command output

Field	Description
RIB GR state	RIB GR status: • **Start**—GR starts. • **IGP end**—All IGP protocols complete GR. • **Routing protocol end**—All routing protocols complete GR.

Field	Description
	• **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Triggering start**—All triggered optimal route selection starts. • **Triggering end**—All triggered optimal route selection completes. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **All end**—All protocols complete GR. • **Phase2-calculation end**—Optimal route selection phase 2 completes.
RCOM GR state	RCOM GR status: • **Start**—GR starts. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **Notification end**—All routes have been delivered to the route management module. • **Phase2-calculation end**—Optimal route selection phase 2 completes. • **Flush start**—Starts to flush routes to the FIB. • **Flush end**—Completes flushing routes to the FIB.
No.	Protocol number.
Lifetime	Lifetime (in seconds) of routes in the RIB during GR.
FD	Handle between the protocol and the RIB.
State	Protocol GR state: • **Init**—Initialization state. • **Listen**—Listening state. • Idle. • Active. • **Start**—GR starts. • **End**—GR completes.
Start/End	Message sending state: • **No**—The message has not been sent. • **Yes**—The message has been sent.

display rib nib

Use **display rib nib** to display next hop information in the RIB.

Syntax

display rib nib [**self-originated**] [*nib-id*] [**verbose**]

display rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`self-originated`: Displays information about next hops of self-originated routes in the RIB.

`nib-id`: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

`verbose`: Displays detailed next hop information in the RIB. If you do not specify this keyword, the command displays brief next hop information in the RIB.

`protocol` *`protocol`*: Specifies a protocol by its name.

Examples

Display brief next hop information in the RIB.

```
<Sysname> display rib nib
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111            LocalAddr: 0.0.0.0
   TopoNthp: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112            LocalAddr: 127.0.0.1
   TopoNthp: 0

      NibID: 0x10000002        Sequence: 2
       Type: 0x5                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112            LocalAddr: 127.0.0.1
   TopoNthp: 0

      NibID: 0x16000000        Sequence: 3
       Type: 0x21               Flushed: No
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 12.1.1.2
    IFIndex: 0x0              LocalAddr: 0.0.0.0
   TopoNthp: 0
   Instance: abc

...
```

Table 10 Command output

Field	Description
NibID	ID of the next hop.
Sequence	Sequence number of the next hop.
Type	Type of the next hop.
Flushed	Indicates whether the route with the next hop has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support non-base topologies.

Display detailed next hop information in the RIB.

```
<Sysname> display rib nib verbose
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111            LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 6              FlushRefCnt: 2
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
  RelyDepth: 0              RealNexthop: 0.0.0.0
  Interface: NULL0            LocalAddr: 0.0.0.0
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112            LocalAddr: 127.0.0.1
```

```
   TopoNthp: 0
     RefCnt: 11             FlushRefCnt: 5
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
  RelyDepth: 0              RealNexthop: 127.0.0.1
  Interface: InLoop0          LocalAddr: 127.0.0.1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0

      NibID: 0x15000003        Sequence: 3
       Type: 0x43               Flushed: Yes
   UserKey0: 0x100010000        VrfNthp: 0
   UserKey1: 0x0                Nexthop: 22.22.22.22
    IFIndex: 0x0              LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 9              FlushRefCnt: 3
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 22.22.22.22
  RelyDepth: 1              RealNexthop: 13.1.1.2
  Interface: Vlan11           LocalAddr: 13.1.1.1
  TunnelCnt: 1                      Vrf: default-vrf
   TunnelID: 1025              Topology: base
     Weight: 0

...
```

Table 11 Command output

Field	Description
x nexthop (s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
LocalAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version.

Field	Description
	Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support non-base topologies.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

display route-direct nib

Use **`display route-direct nib`** to display next hop information for direct routes.

Syntax

`display route-direct nib` [*`nib-id`*] [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`nib-id`: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

`verbose`: Displays detailed next hop information for direct routes. If you do not specify this keyword, the command displays brief next hop information for direct routes.

Examples

Display brief next hop information for direct routes.

```
<Sysname> display route-direct nib
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
```

```
    IFIndex: 0x112           LocalAddr: 127.0.0.1
   TopoNthp: 0

...
```

Table 12 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface IP address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support non-base topologies.

Display detailed next hop information for direct routes.

```
<Sysname> display route-direct nib verbose
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 2              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
  RelyDepth: 0              RealNexthop: 0.0.0.0
  Interface: NULL0            LocalAddr: 0.0.0.0
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0

      NibID: 0x10000001        Sequence: 1
```

```
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112            LocalAddr: 127.0.0.1
   TopoNthp: 0
     RefCnt: 5              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
  RelyDepth: 0              RealNexthop: 127.0.0.1
  Interface: InLoop0          LocalAddr: 127.0.0.1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0
...
```

Table 13 Command output

Field	Description
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support non-base topologies.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

fib lifetime

Use **fib lifetime** to set the maximum lifetime for IPv4 or IPv6 routes in the FIB.

Use **undo fib lifetime** to restore the default.

Syntax

fib lifetime *seconds*

undo fib lifetime

Default

The maximum lifetime for IPv4 or IPv6 routes in the FIB is 600 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum lifetime for routes in the FIB, in the range of 0 to 6000 seconds. When this argument is set to 0, FIB entries immediately age out after a protocol or RIB process switchover.

Usage guidelines

When a protocol or RIB process switchover occurs and GR or NSR is not configured, FIB entries age out after the time specified in this command.

Examples

Set the maximum lifetime for IPv4 routes in the FIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] fib lifetime 60
```

inter-protocol fast-reroute

Use **inter-protocol fast-reroute** to enable IPv4 or IPv6 RIB inter-protocol FRR.

Use **undo inter-protocol fast-reroute** to disable IPv4 or IPv6 RIB inter-protocol FRR.

Syntax

inter-protocol fast-reroute

undo inter-protocol fast-reroute

Default

Inter-protocol FRR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Usage guidelines

This command allows a device to perform fast rerouting between routes of different protocols. A backup next hop is automatically selected to reduce the service interruption time caused by unreachable next hops. When the next hop of the primary link fails, the traffic is redirected to the backup next hop.

This command uses the next hop of a route from a different protocol as the backup next hop for the faulty route, which might cause loops.

Inter-protocol FRR cannot select a backup next hop from routes in the RIB that have the same next hop, output interface, and destination as those of the faulty route.

Examples

Enable IPv4 RIB inter-protocol FRR for the public network.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] inter-protocol fast-reroute
```

max-ecmp-num

Use **max-ecmp-num** to set the maximum number of IPv4 ECMP routes.

Syntax

max-ecmp-num *number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes

Hardware series	Model	Product code	Command compatibility
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-L-PWR • WX3024H • WX3024H-L-PWR • WX3024H-F No: WX3010H-X-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

Default

The device supports a maximum of four IPv4 ECMP routes.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of IPv4 ECMP routes.

Examples

Set the maximum number of IPv4 ECMP routes to 10.

```
<Sysname> system-view
[Sysname] max-ecmp-num 10
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

After reboot, the maximum number of IPv4 ECMP routes is 10.

non-stop-routing

Use **non-stop-routing** to enable RIB NSR.

Use **undo non-stop-routing** to disable RIB NSR.

Syntax

non-stop-routing

undo non-stop-routing

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	No
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	No
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	No
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	No

Hardware series	Model	Product code	Command compatibility
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Command compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	No
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

Default

RIB NSR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Examples

Enable NSR for the RIB IPv4 address family.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] non-stop-routing
```

protocol lifetime

Use **protocol lifetime** to set the maximum lifetime for IPv4 or IPv6 routes in the RIB.

Use **undo protocol lifetime** to restore the default.

Syntax

protocol *protocol* **lifetime** *seconds*

undo protocol *protocol* **lifetime**

Default

The maximum lifetime for IPv4 or IPv6 routes in the RIB is 480 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol.

seconds: Specifies the maximum lifetime for routes in the RIB, in the range of 1 to 6000 seconds.

Usage guidelines

When GR is enabled, make sure the protocol can complete GR and install all route entries to the RIB within the lifetime configured in this command.

Examples

Set the maximum lifetime for RIP routes in the RIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] protocol rip lifetime 60
```

reset ip routing-table statistics protocol

Use **reset ip routing-table statistics protocol** to clear IPv4 route statistics.

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

protocol: Clears route statistics for a routing protocol.

all: Clears route statistics for all IPv4 routing protocols.

Usage guidelines

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv4 route statistics for the public network.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics protocol

Use **reset ipv6 routing-table statistics protocol** to clear IPv6 route statistics.

Syntax

reset ipv6 routing-table statistics protocol { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

protocol: Clears route statistics for an IPv6 routing protocol.

all: Clears route statistics for all IPv6 routing protocols.

Usage guidelines

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv6 route statistics for the public network.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

rib

Use **rib** to enter RIB view.

Use **undo rib** to remove all configurations in RIB view.

Syntax

rib

undo rib

Views

System view

Predefined user roles

network-admin

Examples

Enter RIB view.

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

Contents

Basic IP forwarding commands ····· 1
display fib ····· 1
Load sharing commands ····· 3
ip load-sharing mode ····· 4

Basic IP forwarding commands

display fib

Use **display fib** to display FIB entries.

Syntax

display fib [*ip-address* [*mask* | *mask-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Displays the FIB entry that matches the specified destination IP address.

mask: Specifies the mask for the IP address.

mask-length: Specifies the mask length for the IP address. The value range is 0 to 32.

Usage guidelines

If you specify an IP address without a mask or mask length, this command displays the longest matching FIB entry.

If you specify an IP address and a mask or mask length, this command displays the exactly matching FIB entry.

Examples

Display all FIB entries of the public network.

```
<Sysname> display fib

Destination count: 5 FIB entry count: 5

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
1.1.1.0/24         192.168.126.1   USGF     M-GE0/0/0                Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
127.0.0.1/32       127.0.0.1       UH       InLoop0                  Null
```

Display the FIB entries matching the destination IP address 10.2.1.1.

```
<Sysname> display fib 10.2.1.1

Destination count: 1 FIB entry count: 1
```

```
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
10.2.1.1/32        127.0.0.1       UH       InLoop0                  Null
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of FIB entries.
Destination/Mask	Destination address and the mask length.
Nexthop	Next hop address.
Flag	Flags of routes: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Blackhole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Relay route. • **F**—Fast reroute.
OutInterface/Token	Output interface/LSP index number.
Label	Inner label.

Load sharing commands

The following compatibility matrixes show the support of hardware platforms for loading sharing:

Hardware series	Model	Product code	Loading sharing compatibility
WX1800H series	WX1804H	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-X • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	Loading sharing compatibility
WX1800H series	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	No
WX5800H series	WX5860H	EWP-WX5860H-GL	No

ip load-sharing mode

Use **ip load-sharing mode** to configure the load sharing mode.

Use **undo ip load-sharing mode** to restore the default.

Syntax

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] * | **per-packet** } **global**

undo ip load-sharing mode global

Default

The device performs per-flow load sharing.

Views

System view

Predefined user roles

network-admin

Parameters

per-flow: Implements per-flow load sharing.

dest-ip: Identifies flows by destination IP address.

dest-port: Identifies flows by destination port.

ip-pro: Identifies flows by protocol number.

src-ip: Identifies flows by source IP address.

src-port: Identifies flows by source port.

global: Configures the load sharing mode globally.

per-packet: Implements per-packet load sharing.

Usage guidelines

The per-packet load sharing mode does not take effect in fast forwarding.

Examples

Configure per-flow load sharing.

```
<Sysname> system-view
[Sysname] ip load-sharing mode per-flow global
```

Contents

Static routing commands 1
delete static-routes all 1
display route-static nib 1
display route-static routing-table 5
ip route-static 7
ip route-static default-preference 9
ip route-static fast-reroute auto 10
ip route-static-group 10
prefix 11

Static routing commands

delete static-routes all

Use **delete static-routes all** to delete all static routes.

Syntax

delete static-routes all

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:
This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the static routes.

To delete one static route, use the **undo ip route-static** command. To delete all static routes, including the default route, use the **delete static-routes all** command.

Examples

Delete all static routes.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all IPv4 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip route-static

display route-static nib

Use **display route-static nib** to display static route next hop information.

Syntax

display route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string of 1 to ffffffff. If you do not specify this argument, the command displays all static route next hop information.

verbose: Displays detailed static route next hop information. If you do not specify this keyword, the command displays brief static route next hop information.

Examples

Displays brief static route next hop information.

```
<Sysname> display route-static nib
Total number of nexthop(s): 44

     NibID: 0x11000000       Sequence: 0
      Type: 0x21             Flushed: Yes
  UserKey0: 0x111             VrfNthp: 0
  UserKey1: 0x0               Nexthop: 0.0.0.0
   IFIndex: 0x111           LocalAddr: 0.0.0.0
  TopoNthp: 0

     NibID: 0x11000001       Sequence: 1
      Type: 0x41             Flushed: Yes
  UserKey0: 0x0               VrfNthp: 5
  UserKey1: 0x0               Nexthop: 2.2.2.2
   IFIndex: 0x0             LocalAddr: 0.0.0.0
  TopoNthp: 0

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.

Field	Description
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the public network.

Displays detailed static route next hop information.

```
<Sysname> display route-static nib verbose
Total number of nexthop(s): 44

     NibID: 0x11000000      Sequence: 0
      Type: 0x21            Flushed: Yes
   UserKey0: 0x111           VrfNthp: 0
   UserKey1: 0x0             Nexthop: 0.0.0.0
    IFIndex: 0x111         LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 2           FlushRefCnt: 0
       Flag: 0x2            Version: 1
 1 nexthop(s):
PrefixIndex: 0           OrigNexthop: 0.0.0.0
  RelyDepth: 0           RealNexthop: 0.0.0.0
  Interface: NULL0         LocalAddr: 0.0.0.0
  TunnelCnt: 0                 Vrf: default-vrf
   TunnelID: N/A           Topology: base
     Weight: 1000000

     NibID: 0x11000001      Sequence: 1
      Type: 0x41            Flushed: Yes
   UserKey0: 0x0             VrfNthp: 5
   UserKey1: 0x0             Nexthop: 2.2.2.2
    IFIndex: 0x0           LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 1           FlushRefCnt: 0
       Flag: 0x12           Version: 1
 2 nexthop(s):
PrefixIndex: 0           OrigNexthop: 2.2.2.2
  RelyDepth: 7           RealNexthop: 8.8.8.8
  Interface: Vlan11        LocalAddr: 12.12.12.12
  TunnelCnt: 0                 Vrf: default-vrf
   TunnelID: N/A           Topology: base
     Weight: 1000000
PrefixIndex: 0           OrigNexthop: 2.2.2.2
  RelyDepth: 9           RealNexthop: 0.0.0.0
  Interface: NULL0         LocalAddr: 0.0.0.0
  TunnelCnt: 0                 Vrf: default-vrf
   TunnelID: N/A           Topology: base
```

```
    Weight: 1000000

...
```

Table 2 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
UserKey1	Reserved data 2.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the public network.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
OrigNexthop	Original next hop.
RelyDepth	Recursion depth.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
TunnelCnt	Number of tunnels after route recursion.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the public network is

Field	Description
	base.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.

display route-static routing-table

Use **display route-static routing-table** to display static routing table information.

Syntax

display route-static routing-table [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies the destination IP address in dotted decimal notation. If you do not specify this argument, the command displays all static routing table information.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Examples

Display static routing table information.

```
<Sysname> display route-static routing-table
Total number of routes: 24

Status: * - valid

*Destination: 0.0.0.0/0
      NibID: 0x1100000a       NextHop: 2.2.2.10
   MainNibID: N/A           BkNextHop: N/A
     BkNibID: N/A           Interface: Vlan-interface11
     TableID: 0x2         BkInterface: Vlan-interface12
        Flag: 0x82d01        BfdSrcIp: N/A
     DbIndex: 0xd          BfdIfIndex: 0x0
        Type: Normal       BfdVrfIndex: 0
  TrackIndex: 0xffffffff        Label: NULL
  Preference: 60          vrfIndexDst: 0
     BfdMode: N/A          vrfIndexNH: 0
   Permanent: 0                  Tag: 0

 Destination: 0.0.0.0/0
```

```
     NibID: 0x1100000b        NextHop: 2.2.2.11
  MainNibID: N/A            BkNextHop: N/A
    BkNibID: N/A            Interface: Vlan-interface13
    TableID: 0x2          BkInterface: Vlan-interface14
       Flag: 0x82d01         BfdSrcIp: N/A
    DbIndex: 0xd           BfdIfIndex: 0x0
       Type: Normal        BfdVrfIndex: 0
 TrackIndex: 0xffffffff          Label: NULL
 Preference: 60            vrfIndexDst: 0
    BfdMode: N/A           vrfIndexNH: 0
  Permanent: 0                   Tag: 0
```

...

Table 3 Command output

Field	Description
destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.
TableID	ID of the table to which the route belongs.
Flag	Flag of the route.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT. • IPsec.
BfdSrcIp	This field is not supported in the current software version. Source IP address of the indirect BFD session.
BfdIfIndex	This field is not supported in the current software version. Index of the interface where BFD is enabled.
BfdVrfIndex	This field is not supported in the current software version. Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the public network.
BfdMode	This field is not supported in the current software version. BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode • **Echo**—Echo packet mode.

Field	Description
TrackIndex	NQA Track index.
Label	Label.
vrfIndexDst	This field is not supported in the current software version. Index of VPN instance that the destination belongs to. For the public network, this field displays **0**.
vrfIndexNH	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. For the public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ip route-static

Use **ip route-static** to configure a static route.

Use **undo ip route-static** to delete a static route.

Syntax

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } *interface-type interface-number* [*next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } *next-hop-address* [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference*]

Default

No static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

group *group-name*: Specifies a static route group by its name, a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Specifies an output interface by its type and number. For more information, see *Layer 3—IP Routing Configuration Guide*.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation. For more information, see *Layer 3—IP Routing Configuration Guide*.

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the backup output interface is an NBMA interface or broadcast interface and not a P2P interface, you must specify the backup next hop address.

backup-nexthop *backup-nexthop-address*: Specifies a backup next hop address.

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

track *track-entry-number*: Associates the static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *High Availability Configuration Guide*.

preference *preference*: Specifies a preference for the static route, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag value for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies.

description *text*: Configures a description of 1 to 60 characters for the static route. The description can include special characters, such as the space, except the question mark (?).

Usage guidelines

If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route is used for forwarding a packet matching no entry in the routing table.

Implement different routing policies to configure different route preferences. For example, to enable load sharing for multiple routes to the same destination, assign the same preference to the routes. To enable the routes to back up one another, assign different preferences to them. Only the WX2540E and WX2540H access controllers support load sharing and route backup.

Follow these guidelines when you specify the output interface or the next hop address of the static route:

- If the output interface is a Null 0 interface, no next hop address is required.
- If the output interface is a point-to-point interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.

- Multiple next hops might exist if the output interface is a broadcast interface (for example, an Ethernet interface or VLAN interface). You must specify both the output interface and next hop IP address for the static route.

If you specify a static route group, all prefixes in the static route group will be assigned the next hop and output interface specified by using this command.

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**.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet
```

Related commands

display ip routing-table protocol

ip route-static-group

prefix

ip route-static default-preference

Use **ip route-static default-preference** to configure a default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

Syntax

ip route-static default-preference *default-preference*

undo ip route-static default-preference

Default

The default preference of static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for a static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added static routes.

Examples

Set a default preference of 120 for static routes.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

Related commands

display ip routing-table protocol

ip route-static fast-reroute auto

Use **ip route-static fast-reroute auto** to configure static route FRR to automatically select a backup next hop.

Use **undo ip route-static fast-reroute auto** to disable static route FRR from automatically selecting a backup next hop.

Syntax

ip route-static fast-reroute auto

undo ip route-static fast-reroute auto

Default

Static route FRR is disabled from automatically selecting a backup next hop.

Views

System view

Predefined user roles

network-admin

Examples

Configure static route FRR to automatically select a backup next hop.

```
<Sysname> system-view
[Sysname] ip route-static fast-reroute auto
```

ip route-static-group

Use **ip route-static-group** to create a static route group and enter its view, or enter the view of an existing static route group.

Use **undo ip route-static-group** to delete a static route group.

Syntax

ip route-static-group *group-name*

undo ip route-static-group *group-name*

Default

No static route groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the static route group name, a case-sensitive string of 1 to 31 characters.

Examples

Create static route group **test** and enter its view.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test]
```

Related commands

ip route-static

prefix

prefix

Use **prefix** to add a static route prefix to a static route group.

Use **undo prefix** to delete a static route prefix from a static route group.

Syntax

prefix *dest-address* { *mask-length* | *mask* }

undo prefix *dest-address* { *mask-length* | *mask* }

Default

No static route prefix is added to a static route group.

Views

Static route group view

Predefined user roles

network-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Usage guidelines

Execute this command repeatedly to add multiple static route prefixes to a static route group.

After you add static route prefixes to a static route group, you can specify that group in the **ip route-static group** command to configure static routes with the prefixes. To configure more static routes, you only need to add new static route prefixes to the group.

Examples

Add static route prefix 1.1.1.1/32 to static route group **test**.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test] prefix 1.1.1.1 32
```

Related commands

ip route-static

ip route-static-group

Contents

IPv6 static routing commands 1

delete ipv6 static-routes all 1
display ipv6 route-static nib 1
display ipv6 route-static routing-table 4
ipv6 route-static 6
ipv6 route-static default-preference 8

IPv6 static routing commands

delete ipv6 static-routes all

Use **delete ipv6 static-routes all** to delete all IPv6 static routes.

Syntax

delete ipv6 static-routes all

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:
This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the IPv6 static routes.

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
```

Related commands

ipv6 route-static

display ipv6 route-static nib

Use **display ipv6 route-static nib** to display IPv6 static route next hop information.

Syntax

display ipv6 route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed IPv6 static route next hop information. If you do not specify this keyword, the command displays brief IPv6 static route next hop information.

Examples

Display brief IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance to which the next hop belongs. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop.

Field	Description
	This field displays **0** if the next hop is on the public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support non-base topologies.

Display detailed IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib verbose
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 2::3
  RelyDepth: 2              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 3::4
  RelyDepth: 1              RealNexthop: ::
  Interface: Vlan11           LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

Table 2 Command output

Field	Description
x nexthop(s)	Number of next hops.

Field	Description
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. This field is blank for IPv6, because IPv6 does not support non-base topologies.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

display ipv6 route-static routing-table

Use **display ipv6 route-static routing-table** to display IPv6 static routing table information.

Syntax

display ipv6 route-static routing-table [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

Examples

Display IPv6 static routing table information.

```
<Sysname> display ipv6 route-static routing-table
Total number of routes: 5

Status: * - valid

*Destination: 1::1/128
       NibID: 0x21000000        NextHop: 2::2
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: Vlan-interface11
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x3            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

*Destination: 1::1234/128
      NibID: 0x21000000        NextHop: 2::2
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: NULL0
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x1            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

...
```

Table 3 Command output

Field	Description
Destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.

Field	Description
TableID	ID of the table to which the route belongs.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT.
BfdSrcIp	This field is not supported in the current software version. Source IPv6 address of the indirect BFD session.
BfdIfIndex	This field is not supported in the current software version. Index of the interface where BFD is enabled.
BfdVrfIndex	This field is not supported in the current software version. Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the public network.
BfdMode	This field is not supported in the current software version. BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode. • **Echo**—Echo packet mode.
TrackIndex	NQA Track index.
vrfIndexDst	This field is not supported in the current software version. Index of the VPN instance to which the destination belongs. For the public network, this field displays **0**.
vrfIndexNH	This field is not supported in the current software version. Index of the VPN instance to which the next hop belongs. For the public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ipv6 route-static

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**permanent**] | *next-hop-address* [**permanent**] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference*]

Default

No IPv6 static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address prefix-length: Specifies the IPv6 address and prefix length.

interface-type interface-number: Specifies an output interface by its type and number. If the output interface is a non-P2P interface (for example, an NBMA interface or broadcast interface), the next hop address must be specified.

next-hop-address: Specifies the next hop IPv6 address.

permanent: Specifies the IPv6 route as a permanent IPv6 static route. If the output interface is down, the permanent IPv6 static route is still active.

preference *preference*: Specifies a preference for IPv6 static routes, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies.

description *text*: Configures a description for the IPv6 static route, which consists of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

Usage guidelines

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 is used to forward the packet.

You can configure the output interface, next hop address, or both for a static route. If the output interface is a broadcast interface (for example, an Ethernet interface or a VLAN interface), the next hop address must be specified.

Examples

Configure an IPv6 static route, with the destination address 1:1:2::/64 and next hop 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 64 1:1:3::1
```

Related commands

display ipv6 routing-table protocol

ipv6 route-static default-preference

Use **ipv6 route-static default-preference** to set a default preference for IPv6 static routes.

Use **undo ipv6 route-static default-preference** to restore the default.

Syntax

ipv6 route-static default-preference *default-preference*

undo ipv6 route-static default-preference

Default

The default preference of IPv6 static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for IPv6 static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for an IPv6 static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added IPv6 static routes.

Examples

Set a default preference of 120 for IPv6 static routes.

```
<Sysname> system-view
[Sysname] ipv6 route-static default-preference 120
```

Related commands

display ipv6 routing-table protocol

Contents

RIP commands 1

checkzero 2
default cost 2
default-route 3
display rip 4
display rip database 6
display rip graceful-restart 7
display rip interface 7
display rip neighbor 9
display rip route 10
filter-policy export 12
filter-policy import 14
graceful-restart 15
graceful-restart interval 16
host-route 16
import-route 17
maximum load-balancing 18
network 19
output-delay 19
peer 20
preference 21
reset rip process 21
reset rip statistics 22
rip 22
rip authentication-mode 23
rip default-route 24
rip enable 24
rip input 25
rip max-packet-length 26
rip metricin 26
rip metricout 27
rip mib-binding 27
rip output 28
rip output-delay 28
rip poison-reverse 29
rip split-horizon 29
rip summary-address 30
rip version 31
silent-interface 32
summary 32
timers 33
validate-source-address 34
version 34

RIP commands

The following compatibility matrixes show the support of hardware platforms for RIP:

Hardware series	Model	Product code	RIP compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	MAK206 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3010H-X-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	RIP compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	No

checkzero

Use **checkzero** to enable zero field check on RIPv1 messages.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

The zero field check function is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

When the zero field check is enabled, the router discards RIPv1 messages in which zero fields contain non-zero values. If all messages are trustworthy, disable this feature to reduce the workload of the CPU.

Examples

Disable zero field check on RIPv1 messages for RIP process 1.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIP view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 3 for redistributed routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] default cost 3
```

Related commands

import-route

default-route

Use **default-route** to configure all interfaces running a RIP process to advertise a default route with a specified metric to RIP neighbors.

Use **undo default-route** to restore the default.

Syntax

default-route { **only** | **originate** } [**cost** *cost-value*]

undo default-route

Default

No default route is sent to RIP neighbors.

Views

RIP view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

Usage guidelines

A RIP router configured with this feature does not receive any default route from RIP neighbors.

Examples

Configure all interfaces running RIP process 100 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
```

Related commands

rip default-route

display rip

Use **display rip** to display state and configuration information for a RIP process.

Syntax

display rip [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If no process is specified, the command displays state and configuration information for all RIP processes.

Examples

Display current state and configuration information for all RIP processes.

```
<Sysname> display rip
  Public VPN-instance name:
    RIP process: 1
       RIP version: 1
       Preference: 100
           Routing policy: abc
       Checkzero: Enabled
       Default cost: 0
       Summary: Enabled
       Host routes: Enabled
       Maximum number of load balanced routes: 8
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       BFD: Disabled
       Silent interfaces: None
       Default routes: Originate  Default routes cost: 3
       Verify-source: Enabled
       Networks:
           1.0.0.0
       Configured peers:
           197.168.6.2
       Triggered updates sent: 0
```

```
Number of routes changes: 1
Number of replies to queries: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	The RIP process runs on the public network.
RIP process	RIP process ID.
RIP version	RIP version 1 or 2.
Preference	RIP preference.
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages: **Enabled** or **Disabled**.
Default cost	Default cost of redistributed routes.
Summary	Indicates whether route summarization is enabled: **Enabled** or **Disabled**.
Host routes	Indicates whether to receive host routes: **Enabled** or **Disabled**.
Maximum number of load balanced routes	Maximum number of ECMP routes for load balancing.
Update time	RIP update interval, in seconds.
Timeout time	RIP timeout time, in seconds.
Suppress time	RIP suppress interval, in seconds.
Garbage-collect time	RIP garbage-collect interval, in seconds.
Update output delay	RIP packet sending interval, in seconds.
Output count	Maximum number of RIP packets sent at each interval.
Graceful-restart interval	GR interval, in seconds.
Triggered Interval	Triggered update sending interval.
BFD	This field is not supported in the current software version. Whether BFD is enabled: • **Disabled**—Disabled in RIP view. • **Enabled**—Enabled in RIP view. RIP uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. • **Enabled (ctrl)**—Enabled in RIP view. RIP uses BFD bidirectional control detection for both directly and indirectly connected neighbors.
Silent interfaces	Silent interfaces, which do not periodically send updates.
Default routes	Indicates whether a default route is sent to RIP neighbors. • **only**—Only a default route is advertised. • **originate**—A default route is advertised along with other routes. • **disable**—No default route is advertised.

Field	Description
Default routes cost	Metric for a default route.
Verify-source	Indicates whether the source IP address is checked for received RIP routing updates: **Enabled** or **Disabled**.
Networks	Networks enabled with RIP.
Configured peers	Configured neighbors.
Triggered updates sent	Number of triggered updates sent.
Number of routes changes	Number of route changes.
Number of replies to queries	Number of RIP responses.

display rip database

Use **display rip database** to display active routes for a RIP process.

Syntax

display rip *process-id* **database** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays active routes for the specified IP address. If you do not specify this argument, the command displays all actives routes for a RIP process.

Examples

Display active routes for RIP process 100.

```
<Sysname> display rip 100 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 16, interface summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, imported
   2.0.0.0/8, auto-summary
   2.0.0.0/8, cost 1, nexthop 1.1.1.2
```

Display active routes with destination IP address 1.1.1.0 and mask length 24 for RIP process 100.

```
<Sysname> display rip 100 database 1.1.1.0 24
   1.1.1.0/24, cost 16, interface summary
   1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
```

Table 2 Command output

Field	Description
cost	Cost of the route.

Field	Description
auto-summary	Indicates that the route is a RIP automatic summary route.
interface summary	Indicates that the route is a RIP interface summary route.
nexthop	Address of the next hop.
RIP-interface	Direct route on a RIP-enabled interface.
imported	Indicates that the route is redistributed from another routing protocol.

display rip graceful-restart

Use **display rip graceful-restart** to display the GR status for a RIP process.

Syntax

display rip [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the GR status for all RIP processes.

Examples

Display the GR status for RIP process 1.

```
<Sysname> display rip 1 graceful-restart
 RIP process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time : 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in progress. • **Normal**—No GR is in progress or GR has completed.
Graceful Restart period	GR interval.

display rip interface

Use **display rip interface** to display RIP interface information for a RIP process.

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays information about all RIP interfaces for the RIP process.

Examples

Display information about all interfaces for RIP process 1.

```
<Sysname> display rip 1 interface
Total: 1

 Interface: Vlan-interface10
    Address/Mask: 1.1.1.1/24          Version: RIPv1
    MetricIn: 0                       MetricIn route policy: Not designated
    MetricOut: 1                      MetricOut route policy: Not designated
    Split-horizon/Poison-reverse: On/Off  Input/Output: On/On
    Default route: Off
    Update output delay:  20(ms)      Output count: 3
    BFD: Disabled
    Current number of packets/Maximum number of packets: 0/2000
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIP.
Interface	Name of an interface running RIP.
Address/Mask	IP address and mask of the interface.
Version	RIP version running on the interface.
MetricIn	Additional metric added to incoming routes.
MetricOut	Additional metric added to outgoing routes.
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 whether the interface is enabled to receive and send RIP messages: • **on**—Enabled. • **off**—Disabled.

Field	Description
Default route	Indicates whether to send a default route to RIP neighbors: • **Only**—Advertises only a default route. • **Originate**—Advertises both a default route and other routes. • **No-originate**—Advertises only non-default routes. • **Off**—Advertises no default route.
Default route cost	Metric for a default route.
Update output delay	RIP packet sending interval.
Output count	Maximum number of RIP packets that can be sent at each interval.
BFD	This field is not supported in the current software version. Whether BFD for RIP is enabled: • **Disabled**—Disabled in interface view and RIP view. • **Enabled**—Enabled on the RIP interface. The interface uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. • **Enabled (ctrl)**—Enabled on the RIP interface. The interface uses BFD bidirectional control detection for both directly and indirectly connected neighbors. • **Enabled, inherited**—Enabled in RIP view. RIP uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. The RIP interface uses the BFD setting configured in RIP view. • **Enabled (ctrl), inherited**—Enabled in RIP view. RIP uses BFD bidirectional control detection for both directly and indirectly connected neighbors. The RIP interface uses the BFD setting configured in RIP view. • **Enabled (destination)**—Enabled on the RIP interface. The interface uses BFD single-hop echo detection for a specific destination.
Current number of packets /Maximum number of packets	Number of RIP packets to be sent/maximum number of RIP packets that can be sent within a certain interval.

display rip neighbor

Use **`display rip neighbor`** to display neighbor information for a RIP process.

Syntax

`display rip` *`process-id`* **`neighbor`** [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`process-id`: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays all neighbor information for the RIP process.

Examples

Display neighbor information for RIP process 1.

```
<Sysname> display rip 1 neighbor
 Neighbor address: 197.168.2.3
     Interface  : Vlan-interface10
     Version    : RIPv2     Last update: 00h00m02s
     Relay nbr  : N/A       BFD session: N/A
     Bad packets: 0         Bad routes : 0
```

Table 5 Command output

Field	Description
Interface	Output interface that is connected to the neighbor.
Version	Version of RIP that the neighbor runs.
Last update	Time elapsed since the most recent update.
Relay nbr	Relay neighbor type.
BFD session	This field is not supported in the current software version. BFD session type.
Bad packets	Number of received bad packets.
Bad routes	Number of received bad routes.

display rip route

Use **display rip route** to display routing information for a RIP process.

Syntax

display rip *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays route information for the specified IP address.

verbose: Displays all routing information for the specified destination IP address. If you do not specify this keyword, the command displays only information about optimal routes with the specified destination IP address.

peer *ip-address*: Displays route information learned from the specified neighbor.

statistics: Displays route statistics, including the total number of routes and number of routes from each neighbor.

Usage guidelines

If no optional parameters are specified, the **display rip** *process-id* **route** command displays all routing information for a RIP process.

Examples

Display all routing information for RIP process 1.

```
<Sysname> display rip 1 route
 Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      3.0.0.0/8               1.1.1.1          1       0       RAOF    24
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      4.4.4.4/32              0.0.0.0          0       0       RDOF    -
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

Display specified routing information for RIP process 1.

```
<Sysname> display rip 1 route 3.0.0.0 8 verbose
 Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
  Destination/Mask    OrigNexthop/RealNexthop          Cost  Tag   Flags Sec
  3.0.0.0/8           1.1.1.1/1.1.1.1                  1     0     RAOF  16
```

Table 6 Command output

Field	Description
Route Flags	• **R**—RIP route. • **P**—The route never ages out. • **A**—The route is aging. • **S**—The route is suppressed. • **G**—The route is in Garbage-collect state. • **D**—The route is a direct route. • **O**—The route is an optimal route. • **F**—The route has been flushed to the RIB.
Peer *X.X.X.X* on *interface-type interface-number*	Routing information learned from a neighbor on a RIP interface.
Local route	Locally generated direct routes.
Destination/Mask	Destination IP address and subnet mask.
Nexthop	Next hop of the route.
OrigNexthop/RealNexthop	If the route is from a directly connected neighbor, the original next hop is the real next hop. If the route is from an indirectly connected neighbor, the **RealNexthop** field displays the recursive next hop for the route. Otherwise, the field is blank.

Field	Description
Cost	Cost of the route.
Tag	Route tag.
Flags	Route state.
Sec	Remaining time of the timer corresponding to the route state.

Display routing statistics for RIP process 1.

```
<Sysname> display rip 1 route statistics
 Peer                    Optimal/Aging       Optimal/Permanent       Garbage
 1.1.1.1                 1/1                 0/0                     0
 Local                   2/0                 0/0                     0
 Total                   3/1                 0/0                     0
```

Table 7 Command output

Field	Description
Peer	IP address of a neighbor.
Optimal	Total number of optimal routes.
Aging	Total number of aging routes.
Permanent	Total number of routes that never age out.
Garbage	Total number of routes in the Garbage-collection state.
Local	Total number of locally generated direct routes.
Total	Total number of routes learned from all RIP neighbors.

filter-policy export

Use **filter-policy export** to configure RIP to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*interface-type interface-number* | **direct** | **rip** [*process-id*] | **static**]

undo filter-policy export [*interface-type interface-number* | **direct** | **rip** [*process-id*] | **static**]

Default

RIP does not filter redistributed routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

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

direct: Filters direct routes.

rip: Filters routes redistributed from RIP.

process-id: Specifies a process ID of RIP, in the range of 1 to 65535. The default value is 1.

Usage guidelines

You can configure only one filtering policy to filter routes redistributed from a routing protocol or an interface. Without any protocol or interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for a protocol or an interface, use the **undo filter-policy export** command with the protocol or interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Use IP prefix list **abc** to filter redistributed routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 export
```

Related commands

acl (*Security Command Reference*)

import-route

filter-policy import

Use **filter-policy import** to configure RIP to filter received routes.

Use **undo filter-policy import** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

Default

RIP does not filter received routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes based on their next hops.

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

Usage guidelines

You can configure only one filtering policy to filter routes received on an interface. Without any interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for an interface, use the **undo filter-policy import** command with the interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received RIP routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

Use IP prefix list **abc** to filter received RIP routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 import
```

Related commands

acl (*Security Command Reference*)

graceful-restart

Use **graceful-restart** to enable RIP GR.

Use **undo graceful-restart** to disable RIP GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIP GR is disabled.

Views

RIP view

Predefined user roles

network-admin

Examples

Enable GR for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart interval 200
```

host-route

Use **host-route** to enable host route reception.

Use **undo host-route** to disable host route reception.

Syntax

host-route

undo host-route

Default

RIP receives host routes.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

A router might receive many host routes from the same subnet. These routes are not helpful for routing and occupy a large number of resources. To solve this problem, use the **undo host-route** command to disable RIP from receiving host routes.

This command takes effect only for RIPv2 routes.

Examples

Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value* | **tag** *tag*] *

import-route rip [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **tag** *tag*] *

undo import-route { **direct** | **rip** [*process-id* | **all-processes**] | **static** }

Default

RIP does not redistribute routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Enables route redistribution from all RIP processes.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify the **allow-direct** keyword, the networks of the local interfaces are not redistributed.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 0 to 16. The default cost is 0.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 0 to 65535. The default is 0.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ip routing-table protocol** command.

When you execute the **undo** form of the command, per-process setting has higher priority than the all-processes setting.

- The **undo import-route rip all-processes** command cannot remove the setting configured for a process by using the **import-route rip** *process-id* command. To

remove the setting for that process, you must specify the process ID in the **undo** form of the command.

Examples

Redistribute static routes into RIP, and set the cost for redistributed routes to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Related commands

default cost

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of RIP equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of RIP ECMP routes equals the maximum number of ECMP routes, which is configurable by using the **max-ecmp-num** command.

Views

RIP view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of RIP ECMP routes. Load balancing is not implemented when the value is 1. The value range for this argument is 1 to 4.

Usage guidelines

You can set a smaller value for the **max-ecmp-num** command than the current value for the **maximum load-balancing** command. After a reboot, the value for the **maximum load-balancing** command automatically changes to be the same as the value for the **max-ecmp-num** command.

Examples

Set the maximum number of RIP ECMP routes to 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

Related commands

max-ecmp-num

network

Use **network** to enable RIP on an interface attached to a specified network.

Use **undo network** to disable RIP on an interface attached to a specified network.

Syntax

network *network-address* [*wildcard-mask*]

undo network *network-address*

Default

RIP is disabled on an interface.

Views

RIP view

Predefined user roles

network-admin

Parameters

network-address: Specifies a subnet address where an interface resides.

wildcard-mask: Specifies an IP address wildcard mask. A wildcard mask can be thought of as a subnet mask, with 1s and 0s inverted. For example, a wildcard mask of 255.255.255.0 corresponds to a subnet mask of 0.0.0.255. If you do not specify this argument, the command uses the natural mask.

Usage guidelines

RIP runs only on an interface attached to the specified network, which can be configured with a wildcard mask. An interface not on the specified network does not receive or send RIP routes, or advertise its direct routes.

For a single RIP process, the **network** 0.0.0.0 command can enable RIP on all interfaces. If multiple RIP processes exist, the command is not applicable.

If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

Enable RIP process 100 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
```

Related commands

rip enable

output-delay

Use **output-delay** to set the rate at which an interface sends RIP packets.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

An interface sends up to three RIP packets every 20 milliseconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

time: Specifies the sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure all interfaces running RIP process 1 to send up to 10 RIP packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] output-delay 60 count 10
```

peer

Use **peer** to specify a RIP neighbor in the NBMA network, where routing updates destined for the neighbor are only unicasts and not multicast or broadcast.

Use **undo peer** to remove a RIP neighbor.

Syntax

peer *ip-address*

undo peer *ip-address*

Default

RIP does not unicast updates to any neighbor.

Views

RIP view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a RIP neighbor, in dotted decimal notation.

Usage guidelines

Do not use the **peer** *ip-address* command when the neighbor is directly connected. Otherwise, the neighbor might receive both unicast and multicast (or broadcast) messages with the same routing information.

This command must be executed together with the **undo validate-source-address** command, which disables source IP address check on inbound RIP routing updates.

Examples

Configure RIP to unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
```

```
[Sysname-rip-1] peer 202.38.165.1
```

Related commands

validate-source-address

preference

Use **preference** to specify a preference for RIP routes.

Use **undo preference** to restore the default.

Syntax

preference *preference*

undo preference

Default

The preference of RIP routes is 100.

Views

RIP view

Predefined user roles

network-admin

Parameters

preference: Specifies a preference for RIP routes, in the range of 1 to 255. The smaller the value, the higher the preference.

Examples

Set a preference of 120 for RIP routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip process

Use **reset rip process** to reset a RIP process.

Syntax

reset rip *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Reset RIP process 100.

```
<Sysname> reset rip 100 process
Reset RIP process? [Y/N]:y
```

reset rip statistics

Use **reset rip statistics** to clear statistics for a RIP process.

Syntax

reset rip *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Use **rip** to enable RIP and enter RIP view.

Use **undo rip** to disable RIP.

Syntax

rip [*process-id*]

undo rip [*process-id*]

Default

RIP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. The default is 1.

Usage guidelines

You must enable a RIP process before configuring global parameters for it. This restriction does not apply to configuring interface parameters.

If you disable a RIP process, the configured interface parameters become invalid.

Examples

Enable RIP process 1 and enter RIP view.

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

```
[Sysname-rip-1]
```

rip authentication-mode

Use **rip authentication-mode** to configure RIPv2 authentication.

Use **undo rip authentication-mode** to restore the default.

Syntax

rip authentication-mode { **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

undo rip authentication-mode

Default

RIPv2 authentication is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

md5: Specifies MD5 authentication.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Specifies a password in encrypted form.

plain: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

key-id: Specifies the key ID in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

Usage guidelines

A newly configured key overwrites the old one, if any.

Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect because RIPv1 does not support authentication.

Examples

Configure MD5 authentication on VLAN-interface 10 and specify a plaintext key **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 plain rose
```

Related commands

rip version

rip default-route

Use **rip default-route** to configure a RIP interface to advertise a default route with a specified metric.

Use **undo rip default-route** to disable a RIP interface from sending a default route.

Syntax

rip default-route { { **only** | **originate** } **cost** *cost-value* | **no-originate** }

undo rip default-route

Default

A RIP interface advertises a default route if the RIP process that the interface runs is enabled to advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

no-originate: Advertises only non-default routes.

Usage guidelines

An interface that is enabled to advertise a default route does not receive any default route from RIP neighbors.

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
```

Configure VLAN-interface 10 to advertise a default route with a metric of 2 and other routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route originate cost 2
```

Related commands

default-route

rip enable

Use **rip enable** to enable RIP on an interface.

Use **undo rip enable** to disable RIP on an interface.

Syntax

rip *process-id* **enable** [**exclude-subip**]

undo rip enable

Default

RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

exclude-subip: Excludes secondary IP addresses from being enabled with RIP. If you do not specify this keyword, RIP is also enabled on secondary IP addresses of a RIP-enabled interface.

Usage guidelines

The **rip enable** command has a higher priority than the **network** command.

Examples

Enable RIP process 100 on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip 100 enable
```

Related commands

network

rip input

Use **rip input** to enable an interface to receive RIP messages.

Use **undo rip input** to disable an interface from receiving RIP messages.

Syntax

rip input

undo rip input

Default

An interface is enabled to receive RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

rip max-packet-length

Use **rip max-packet-length** to set the maximum length of RIP packets.

Use **undo rip max-packet-length** to restore the default.

Syntax

rip max-packet-length *value*

undo rip max-packet-length

Default

The maximum length of RIP packets is 512 bytes.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum length of RIP packets, in the range of 32 to 65535 bytes.

Usage guidelines

The supported maximum length of RIP packets varies by vendor. Use this feature with caution to avoid compatibility issues.

When authentication is enabled, follow these guidelines to ensure packet forwarding:

- For simple authentication, the maximum length of RIP packets must be no less than 52 bytes.
- For MD5 authentication (with packet format defined in RFC 2453), the maximum length of RIP packets must be no less than 56 bytes.
- For MD5 authentication (with packet format defined in RFC 2082), the maximum length of RIP packets must be no less than 72 bytes.

If the configured value in the **rip max-packet-length** command is greater than the MTU of an interface, the interface MTU value is used as the maximum length of RIP packets.

Examples

Set the maximum length of RIP packets on VLAN-interface 10 to 1024 bytes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip max-packet-length 1024
```

rip metricin

Use **rip metricin** to configure an interface to add a metric to inbound routes.

Use **undo rip metricin** to restore the default.

Syntax

rip metricin *value*

undo rip metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Usage guidelines

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. The metric of the route received on the configured interface is then increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

Examples

rip metricout

Use **rip metricout** to configure an interface to add a metric to outbound routes.

Use **undo rip metricout** to restore the default.

Syntax

rip metricout *value*

undo rip metricout

Default

The additional metric for outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Usage guidelines

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

Examples

rip mib-binding

Use **rip mib-binding** to bind a RIP process to MIB.

Use **undo rip mib-binding** to restore the default.

Syntax

rip mib-binding *process-id*

undo rip mib-binding

Default

MIB operation is bound to the RIP process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration does not take effect.

Deleting a RIP process bound to MIB operation deletes the MIB binding configuration. After the RIP process is deleted, MIB operation is bound to the RIP process with the smallest process ID.

Examples

Bind RIP process 100 to MIB.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

rip output

Use **rip output** to enable an interface to send RIP messages.

Use **undo rip output** to disable an interface from sending RIP messages.

Syntax

rip output

undo rip output

Default

An interface sends RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from sending RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip output-delay

Use **rip output-delay** to set the RIP packet sending interval for an interface and the maximum number of RIP packets that can be sent at each interval.

Use **undo rip output-delay** to restore the default.

Syntax

rip output-delay *time* **count** *count*

undo rip output-delay

Default

An interface uses the RIP packet sending rate set for the RIP process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

Parameters

Time: Specifies the RIP packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure VLAN-interface 10 to send a maximum of six RIP packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip output-delay 30 count 6
```

Related commands

output-delay

rip poison-reverse

Use **rip poison-reverse** to enable the poison reverse feature.

Use **undo rip poison-reverse** to disable the poison reverse feature.

Syntax

rip poison-reverse

undo rip poison-reverse

Default

The poison reverse feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable the poison reverse feature on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip split-horizon

Use **rip split-horizon** to enable the split horizon feature.

Use **undo rip split-horizon** to disable the split horizon feature.

Syntax

rip split-horizon

undo rip split-horizon

Default

The split horizon feature is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The split horizon feature prevents routing loops. If you want to disable the feature, make sure the operation is necessary.

If both split horizon and poison reverse are enabled, only the poison reverse feature takes effect.

Examples

Enable the split horizon feature on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Use **rip summary-address** to configure a summary route on an interface.

Use **undo rip summary-address** to remove a summary route on an interface.

Syntax

rip summary-address *ip-address* { *mask-length* | *mask* }

undo rip summary-address *ip-address* { *mask-length* | *mask* }

Default

No summary route is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the subnet mask length of the summary route, in the range of 0 to 32.

mask: Specifies the subnet mask of the summary route, in dotted decimal notation.

Usage guidelines

This command takes effect only when automatic route summarization is disabled.

Examples

Configure a summary route 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
```

Related commands

summary

rip version

Use **rip version** to specify a RIP version on an interface.

Use **undo rip version** to restore the default.

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Default

No RIP version is configured on an interface. The interface can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

Interface view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2.

[**broadcast** | **multicast**]: Sends RIPv2 messages in broadcast mode or multicast mode (default).

Usage guidelines

If an interface has no RIP version configured, it uses the global RIP version. Otherwise, it uses the RIP version configured on it.

An interface running RIPv1 can perform the following operations:

- Sends RIPv1 broadcast messages.
- Receives RIPv1 broadcast and unicast messages.

An interface running RIPv2 in broadcast mode can perform the following operations:

- Sends RIPv2 broadcast messages.
- Receives RIPv1 broadcast and unicast messages, and RIPv2 broadcast, multicast, and unicast messages.

An interface running RIPv2 in multicast mode can perform the following operations:

- Sends RIPv2 multicast messages.
- Receives RIPv2 broadcast, multicast, and unicast messages.

Examples

Configure RIPv2 in broadcast mode on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] rip version 2 broadcast
```

Related commands

version

silent-interface

Use **silent-interface** to disable interfaces from sending RIP messages. The interfaces can still receive RIP messages.

Use **undo silent-interface** to enable interfaces to send RIP messages.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

All RIP interfaces can send RIP messages.

Views

RIP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Disables a specified interface from sending RIP messages.

all: Disables all interfaces from sending RIP messages.

Examples

Disable all VLAN interfaces from sending RIP messages except 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

Use **summary** to enable automatic RIPv2 route summarization. Natural masks are used to advertise summary routes to reduce the size of routing tables.

Use **undo summary** to disable automatic RIPv2 route summarization to advertise all subnet routes.

Syntax

summary

undo summary

Default

Automatic RIPv2 route summarization is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

Automatic RIPv2 route summarization can reduce the routing table size to enhance the scalability and efficiency for large networks.

Examples

Disable automatic RIPv2 route summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo summary
```

Related commands

rip summary-address

rip version

timers

Use **timers** to set RIP timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

garbage-collect-value: Specifies the garbage-collect timer in the range of 1 to 3600 seconds.

suppress-value: Specifies the suppress timer in the range of 0 to 3600 seconds.

timeout-value: Specifies the timeout timer in the range of 1 to 3600 seconds.

update-value: Specifies the update timer in the range of 1 to 3600 seconds.

Usage guidelines

RIP uses the following timers:

- **Update timer**—Specifies the interval between routing updates.
- **Timeout timer**—Specifies the route aging time. If no update for a route is received before the timer expires, RIP sets the metric of the route to 16.
- **Suppress timer**—Specifies how long a RIP route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIP receives an update for the

route with a metric less than 16 from the same neighbor, RIP uses this route to replace the suppressed route.

- **Garbage-collect timer**—Specifies 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 a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIP deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be consistent on all routers on the network.

The timeout timer must be greater than the update timer.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5, 15, 15, and 30 seconds.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

validate-source-address

Use **validate-source-address** to enable source IP address check on inbound RIP routing updates.

Use **undo validate-source-address** to disable source IP address check on inbound RIP routing updates.

Syntax

validate-source-address

undo validate-source-address

Default

Source IP address check on inbound RIP routing updates is enabled.

Views

RIP view

Predefined user roles

network-admin

Examples

Disable source IP address check on inbound RIP routing updates.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

version

Use **version** to specify a global RIP version.

Use **undo version** to restore the default.

Syntax

version { **1** | **2** }

undo version

Default

No global RIP version is configured. An RIP interface can send RIPv1 broadcasts and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

RIP view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Usage guidelines

An interface prefers the RIP version configured on it over the global RIP version.

If no RIP version is specified for the interface and the global version is RIPv1, the interface uses RIPv1 and can perform the following operations:

- Send RIPv1 broadcasts.
- Receive RIPv1 broadcasts and unicasts.

If no RIP version is specified for the interface and the global version is RIPv2, the interface uses RIPv2 multicast mode and can perform the following operations:

- Send RIPv2 multicasts.
- Receive RIPv2 broadcasts, multicasts, and unicasts.

Examples

Specify the global RIP version as RIPv2.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

Related commands

rip version

Contents

RIPng commands 1

checkzero 2
default cost 2
display ripng 3
display ripng database 4
display ripng graceful-restart 5
display ripng interface 6
display ripng neighbor 7
display ripng route 8
enable ipsec-profile 10
filter-policy export 11
filter-policy import 12
graceful-restart 13
graceful-restart interval 14
import-route 14
maximum load-balancing 15
output-delay 16
preference 17
reset ripng process 18
reset ripng statistics 18
ripng 19
ripng default-route 19
ripng enable 20
ripng ipsec-profile 21
ripng metricin 22
ripng metricout 22
ripng output-delay 23
ripng poison-reverse 24
ripng split-horizon 24
ripng summary-address 25
timers 26

RIPng commands

The following compatibility matrixes show the support of hardware platforms for RIPng:

Hardware series	Model	Product code	RIPng compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3024H • WX3024H-F No: • WX3010H-L-PWR • WX3010H-X-PWR • WX3024H-L-PWR
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	No
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	No
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	No

Hardware series	Model	Product code	RIPng compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	No

checkzero

Use **checkzero** to enable zero field check on RIPng packets.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

Zero field check is enabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable zero field check on incoming RIPng packets. If a zero field of a packet contains a non-zero value, RIPng discards the packet.

Examples

Disable zero field check on RIPng packets for RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIPng view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 2 for redistributed routes.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

Related commands

import-route

display ripng

Use **display ripng** to display state and configuration information for a RIPng process.

Syntax

display ripng [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all RIPng processes.

Examples

Display state and configuration information for all configured RIPng processes.

```
<Sysname> display ripng
  Public VPN-instance name:

RIPng process: 1
       Preference: 100
           Routing policy: abc
       Checkzero: Enabled
       Default cost: 0
       Maximum number of load balanced routes: 6
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       Number of periodic updates sent: 256
       Number of triggered updates sent: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	Public network where the RIPng process runs.
RIPng process	RIPng process ID.
Preference	RIPng preference.
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled: **Enabled** or **Disabled**.
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.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at each interval.
Graceful-restart interval	GR interval in seconds.
Triggered Interval	Triggered update sending interval.

display ripng database

Use **`display ripng database`** to display all active routes in the advertising database for a RIPng process.

Syntax

display ripng *process-id* **database** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display active routes for RIPng process 1.

```
<Sysname> display ripng 1 database
   1::/64,
        cost 0, RIPng-interface
   10::/32,
        cost 0, imported
   2::2/128,
       via FE80::20C:29FF:FE7A:E3E4, cost 1
```

Table 2 Command output

Field	Description
cost	Route metric value.
imported	Indicates the route is redistributed from another routing protocol.
RIPng-interface	Route learned from the interface.
via	Next hop IPv6 address.

display ripng graceful-restart

Use **display ripng graceful-restart** to display GR information.

Syntax

display ripng [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Display GR information for RIPng process 1.

```
<Sysname> display ripng 1 graceful-restart
RIPng process: 1
 Graceful Restart capability    : Enabled
 Current GR state               : Normal
 Graceful Restart period        : 60  seconds
 Graceful Restart remaining time: 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in process. • **Normal**—GR is not in progress or has completed.

display ripng interface

Use **display ripng interface** to display interface information for a RIPng process.

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all interfaces for the RIPng process.

Examples

Display interface information for RIPng process 1.

```
<Sysname> display ripng 1 interface
Total: 1
```

```
Interface: Vlan-interface100
        Link-local address: FE80::20C:29FF:FEC8:B4DD
        Split-horizon: On                Poison-reverse: Off
        MetricIn: 0                      MetricOut: 1
        Default route: Off
        Update output delay: 20 (ms)     Output count: 3
        Summary address:
               1::/16
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIPng.
Interface	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng.
Split-horizon	Indicates whether split horizon is enabled: • **On**—Enabled. • **Off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **On**—Enabled. • **Off**—Disabled.
MetricIn/MetricOut	Additional metric to incoming and outgoing routes.
Default route	• **Only**—The interface advertises only a default route. • **Originate**—The interface advertises a default route and other RIPng routes. • **Off**—In this state, the interface does not advertise a default route. • **In garbage-collection status**—In this state, the interface advertises a default route with a metric of 16.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at each interval.
Default route cost	Cost of the default route.

display ripng neighbor

Use **`display ripng neighbor`** to display neighbor information for a RIPng process.

Syntax

`display ripng` *`process-id`* **`neighbor`** [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all neighbors for the RIPng process.

Examples

Display neighbor information for RIPng process 1.

```
<Sysname> display ripng 1 neighbor
Neighbor Address: FE80::230:FF:FE00:0
     Interface  : Vlan-interface1
     Version    : RIPng version 1     Last update: 00h00m27s
     Bad packets: 0                   Bad routes : 0
```

Table 5 Command output

Field	Description
Neighbor Address	Link-local address of a neighbor interface.
Interface	Name of a neighbor interface.
Version	Version of RIPng that a neighbor runs.
Last update	Time elapsed since the most recent update.

display ripng route

Use **display ripng route** to display all RIPng routes for a RIPng process.

Syntax

display ripng *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

verbose: Displays all routing information for the specified destination IPv6 address. If you do not specify this keyword, the command displays only optimal RIPng routes with the specified destination IPv6 address.

peer *ipv6-address*: Specifies a neighbor by its IPv6 address.

statistics: Displays routing information statistics, including total number of routes and the number of routes learned from each neighbor.

Examples

Display routing information for RIPng process 1.

```
<Sysname> display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------

 Peer FE80::20C:29FF:FED4:7171 on Vlan-interface100
 Destination 4::4/128,
     via FE80::20C:29FF:FED4:7171, cost 1, tag 0, AOF, 5 secs
 Local route
 Destination 3::3/128,
     via ::, cost 0, tag 0, DOF
 Destination 6::/64,
     via ::, cost 0, tag 0, DOF
```

Display information about routes with the specified prefix for RIPng process 1.

```
<Sysname> display ripng 1 route 3::3 128 verbose
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------
 Peer FE80::4283:59FF:FE97:205 on Vlan-interface100
 Destination 3::3/128,
     via FE80::4283:59FF:FE97:205, cost 1, tag 0, AOF, 28 secs
```

Table 6 Command output

Field	Description
A–Aging	The route is in aging state.
S–Suppressed	The route is in suppressed state.
G–Garbage-collect	The route is in Garbage-collect state.
D–Direct	The route is a direct route.
Local route	The route is a locally generated direct route.
O - Optimal	The route is an optimal route.
F - Flush to RIB	The route has been flushed to the RIB.
Peer	Neighbor connected to the interface.
Destination	IPv6 destination address.
via	Next hop IPv6 address.

Field	Description
cost	Routing metric value.
tag	Route tag.
secs	Time a route entry has stayed in the current state.

Display routing information statistics for RIPng process 1.

```
<Sysname> display ripng 1 route statistics
Peer                                          Optimal/Aging    Garbage
 FE80::20C:29FF:FED4:7171                      1/2              0
 Local                                         2/0              0
 total                                         3/2              0
```

Table 7 Command output

Field	Description
Peer	IPv6 address of the neighbor.
Optimal	Number of optimal routes.
Aging	Number of routes in aging state.
Garbage	Number of routes in Garbage-collection state.
Local	Total number of locally generated direct route.
total	Total number of routes learned from RIPng neighbors.

enable ipsec-profile

Use **enable ipsec-profile** to apply an IPsec profile to a RIPng process.

Use **undo enable ipsec-profile** to remove the IPsec profile from the RIPng process.

Syntax

enable ipsec-profile *profile-name*

undo enable ipsec-profile

Default

No IPsec profile is applied to a RIPng process.

Views

RIPng view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] enable ipsec-profile profile001
```

filter-policy export

Use **filter-policy export** to configure RIPng to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

RIPng does not filter redistributed routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from a routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **ripng**. The default is 1.

Usage guidelines

If the *protocol* argument is specified, RIPng filters only routes redistributed from the specified routing protocol. Otherwise, RIPng filters all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the prefix configuration to take effect, specify a contiguous prefix.

Examples

Use IPv6 prefix list to filter redistributed RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc export
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 export
```

filter-policy import

Use **filter-policy import** to configure RIPng to filter received routes.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

Default

RIPng does not filter received routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Examples

Use the IPv6 prefix list **abc** to filter received RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc import
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 import
```

graceful-restart

Use **graceful-restart** to enable Graceful Restart (GR) for RIPng.

Use **undo graceful-restart** to disable RIPng GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIPng GR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Examples

Enable GR for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIPng view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart interval 200
```

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value*]

undo import-route { **direct** | **static** }

import-route ripng [*process-id*] [**allow-direct** | **cost** *cost-value*] *

undo import-route ripng [*process-id*]

Default

RIPng does not redistribute routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. The default is 1.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed.

cost *cost-value*: Specifies a metric for redistributed routes, in the range of 0 to 16. The default metric is 0.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ipv6 routing-table protocol** command.

Examples

Redistribute routes from RIPngprocess 7 into RIPng and set the metric for redistributed routes to 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route ripng7 cost 7
```

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of RIPng ECMP routes equals the maximum number of ECMP routes, which is configurable by using the **max-ecmp-num** command.

Views

RIPng view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ECMP routes. When this argument takes a value of 1, RIPng does not perform load balancing. The value range for this argument is 1 to 4.

Usage guidelines

You can set a smaller value for the **max-ecmp-num** command than the current value for the **maximum load-balancing** command. After a reboot, the value for the **maximum load-balancing** command automatically changes to be the same as the value for the **max-ecmp-num** command.

Examples

Set the maximum number of ECMP routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Related commands

max-ecmp-num

output-delay

Use **output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent at each interval.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

A RIPng process sends a maximum of three RIPng packets every 20 milliseconds.

Views

RIPng view

Predefined user roles

network-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent by a RIPng process at each interval, in the range of 1 to 30.

Usage guidelines

If you configure the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure RIPng process 1 to send a maximum of 10 RIPng packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] output-delay 60 count 10
```

Related commands

ripng output-delay

preference

Use **preference** to set the preference for RIPng routes.

Use **undo preference** to restore the default.

Syntax

preference *preference*

undo preference

Default

The preference of RIPng routes is 100.

Views

RIPng view

Predefined user roles

network-admin

Parameters

preference: Specifies the preference for RIPng routes, in the range of 1 to 255. The smaller the value, the higher the preference.

Examples

Set the preference for RIPng routes to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

reset ripng process

Use **reset ripng process** to restart a RIPng process.

Syntax

reset ripng *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Restart RIPng process 100.

```
<Sysname> reset ripng 100 process
Reset RIPng process? [Y/N]:y
```

reset ripng statistics

Use **reset ripng statistics** to clear statistics for a RIPng process.

Syntax

reset ripng *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIPng process 100.

```
<Sysname> reset ripng 100 statistics
```

ripng

Use **ripng** to enable RIPng and enter RIPng view.

Use **undo ripng** to disable RIPng.

Syntax

ripng [*process-id*]

undo ripng [*process-id*]

Default

RIPng is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. The default value is 1.

Usage guidelines

Before you configure global RIPng parameters, you must create a RIPng process. This restriction does not apply to configuring interface RIPng parameters.

If you disable a RIPng process, the configured RIPng parameters become invalid.

Examples

Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

ripng default-route

Use **ripng default-route** to configure a RIPng interface to advertise a default route with a specified metric.

Use **undo ripng default-route** to disable a RIPng interface from sending a default route.

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost-value*]

undo ripng default-route

Default

A RIPng process does not advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only an IPv6 default route (::/0).

originate: Advertises an IPv6 default route (::/0) and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

Usage guidelines

This command enables the interface to advertise a RIPng default route in a route update regardless of whether the default route exists in the local IPv6 routing table.

A RIPng interface configured to advertise a default route does not receive any default routes from its neighbors.

Examples

Configure RIPng on VLAN-interface 100 to advertise only a default route.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

Configure RIPng on VLAN-interface 101 to advertise a default route and other routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Use **ripng enable** to enable RIPng on an interface.

Use **undo ripng enable** to disable RIPng on an interface.

Syntax

ripng *process-id* **enable**

undo ripng enable

Default

RIPng is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Enable RIPng 100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng ipsec-profile

Use **ripng ipsec-profile** to apply an IPsec profile to a RIPng interface.

Use **undo ripng ipsec-profile** to remove the IPsec profile from the RIPng interface.

Syntax

ripng ipsec-profile *profile-name*

undo ripng ipsec-profile

Default

No IPsec profile is applied to a RIPng interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng ipsec-profile profile001
```

ripng metricin

Use **ripng metricin** to configure an interface to add a metric to inbound RIPng routes.

Use **undo ripng metricin** to restore the default.

Syntax

ripng metricin *value*

undo ripng metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Examples

Configure VLAN-interface 100 to add a metric of 12 to inbound RIPng routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Use **ripng metricout** to configure an interface to add a metric to outbound RIPng routes.

Use **undo ripng metricout** to restore the default.

Syntax

ripng metricout *value*

undo ripng metricout

Default

The additional metric of outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Examples

Configure RIPng on VLAN-interface 100 to add a metric of 12 to outbound routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng output-delay

Use **ripng output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent by an interface at each interval.

Use **undo ripng output-delay** to restore the default.

Syntax

ripng output-delay *time* **count** *count*

undo ripng output-delay

Default

An interface uses the RIPng packet sending rate set for the RIPng process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent at each interval, in the range of 1 to 30.

Usage guidelines

If you set the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure VLAN-interface 100 to send a maximum of six RIPng packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng output-delay 30 count 6
```

Related commands

output-delay

ripng poison-reverse

Use **ripng poison-reverse** to enable poison reverse.

Use **undo ripng poison-reverse** to disable poison reverse.

Syntax

ripng poison-reverse

undo ripng poison-reverse

Default

Poison reverse is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable poison reverse 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

Use **ripng split-horizon** to enable split horizon.

Use **undo ripng split-horizon** to disable split horizon.

Syntax

ripng split-horizon

undo ripng split-horizon

Default

Split horizon is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Split horizon prevents routing loops. If you want to disable this feature, make sure the operation is indispensable.

If both poison reverse and split horizon are enabled, only poison reverse takes effect.

Examples

Enable split horizon on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Use **ripng summary-address** to configure a summary network to be advertised through an interface.

Use **undo ripng summary-address** to remove a summary network.

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

Default

No summary network is configured to be advertised through an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the 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.

Usage guidelines

Networks on the summary network will not be advertised. The cost of the summary route 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.

```
<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

Use **timers** to set RIPng timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIPng view

Predefines user roles

network-admin

Parameters

garbage-collect-value: Sets the garbage-collect timer in the range of 1 to 86400 seconds.

suppress-value: Sets the suppress timer in the range of 0 to 86400 seconds.

timeout-value: Sets the timeout timer in the range of 1 to 86400 seconds.

update-value: Sets the update timer in the range of 1 to 86400 seconds.

Usage guidelines

RIPng has the following timers:

- **Update timer**—Interval between update messages.
- **Timeout timer**—Route aging time. If no update for a route is received before the timer expires, RIPng sets the metric of the route to 16.
- **Suppress timer**—How long a RIPng route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIPng receives an update for the route from the same neighbor and the route in the update has a metric less than 16, RIPng uses the route to replace the suppressed route.
- **Garbage-collect timer**—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 a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIPng deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be kept consistent on all routers in the network.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5 seconds, 15 seconds, 15 seconds, and 30 seconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

Contents

IGMP snooping commands 1

display igmp-snooping 2
display igmp-snooping group 4
display igmp-snooping router-port 6
display igmp-snooping static-group 7
display igmp-snooping static-router-port 8
display igmp-snooping statistics 9
display l2-multicast fast-forwarding cache 10
display l2-multicast ip 12
display l2-multicast ip forwarding 13
display l2-multicast mac 14
display l2-multicast mac forwarding 15
dot1p-priority (IGMP-snooping view) 17
drop-unknown (IGMP-snooping view) 17
enable (IGMP-snooping view) 18
entry-limit (IGMP-snooping view) 19
fast-leave (IGMP-snooping view) 19
group-policy (IGMP-snooping view) 20
host-aging-time (IGMP-snooping view) 21
igmp-snooping 22
igmp-snooping dot1p-priority 23
igmp-snooping drop-unknown 23
igmp-snooping enable 24
igmp-snooping fast-leave 25
igmp-snooping general-query source-ip 26
igmp-snooping group-limit 27
igmp-snooping group-policy 27
igmp-snooping host-aging-time 29
igmp-snooping host-join 30
igmp-snooping last-member-query-interval 31
igmp-snooping leave source-ip 31
igmp-snooping max-response-time 32
igmp-snooping overflow-replace 33
igmp-snooping querier 34
igmp-snooping query-interval 34
igmp-snooping report source-ip 35
igmp-snooping router-aging-time 36
igmp-snooping router-port-deny 37
igmp-snooping special-query source-ip 38
igmp-snooping static-group 38
igmp-snooping static-router-port 39
igmp-snooping version 40
last-member-query-interval (IGMP-snooping view) 41
max-response-time (IGMP-snooping view) 41
overflow-replace (IGMP-snooping view) 42
report-aggregation (IGMP-snooping view) 43
reset igmp-snooping group 43
reset igmp-snooping router-port 44
reset igmp-snooping statistics 44
reset l2-multicast fast-forwarding cache 45
router-aging-time (IGMP-snooping view) 46
version (IGMP-snooping view) 46

IGMP snooping commands

The following compatibility matrixes show the support of hardware platforms for IGMP snooping:

Hardware series	Model	Product code	IGMP snooping compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X • WX3024H • WX3024H-F No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Yes

Hardware series	Model	Product code	IGMP snooping compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

display igmp-snooping

Use **display igmp-snooping** to display IGMP snooping status.

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global IGMP snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status in all VLANs.

Examples

Display the global IGMP snooping status and the IGMP snooping status for all VLANs.

```
<Sysname> display igmp-snooping
IGMP snooping information: Global
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
 Dot1p-priority: --

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
```

```
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Dot1p-priority: 2

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Dot1p-priority: --
```

Table 1 Command output

Field	Description
IGMP snooping	IGMP snooping status in a VLAN: • Enabled. • Disabled.
Drop-unknown	Status of dropping unknown multicast data: • Enabled. • Disabled.
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: • Enabled. • Disabled.

Field	Description
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (--).
Querier	Status of IGMP snooping querier: • Enabled. • Disabled.
Query-interval	Interval for sending IGMP general queries.
General-query source IP	Source IP address of IGMP general queries.
Special-query source IP	Source IP address of IGMP group-specific queries.
Report source IP	Source IP address of IGMP reports.
Leave source IP	Source IP address of IGMP leave messages.

display igmp-snooping group

Use **display igmp-snooping group** to display information about dynamic IGMP snooping group entries.

Syntax

In standalone mode:

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]

In IRF mode:

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about dynamic IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about dynamic IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic IGMP snooping group entries for all VLANs.

verbose: Displays detailed information about dynamic IGMP snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic IGMP snooping group entries for the master device. (In IRF mode.)

Examples

Display detailed information about dynamic IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      WLAN-BSS1/0/10                              (00:03:23)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—No entry exists. • **normal**—The entry is a correct entry.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports, and the total number of member ports.
(00:03:23)	Remaining aging time for the dynamic member port. For a global port, this field is always displayed. (In standalone mode.) For a non-global port, this field is always displayed. (In IRF mode.) For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset igmp-snooping group

display igmp-snooping router-port

Use **display igmp-snooping router-port** to display dynamic router port information.

Syntax

In standalone mode:

display igmp-snooping router-port [**verbose** | **vlan** *vlan-id*]

In IRF mode:

display igmp-snooping router-port [**verbose** | **vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information. If you do not specify the keyword, this command displays brief information.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device. (In IRF mode.)

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router ports (1 in total):
    WLAN-BSS1/0/10                          (00:01:30)
```

Table 3 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (1 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. For a global port, this field is always displayed. (In standalone mode.) For a global port, this field is always displayed. (In IRF mode.) For a global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device.

Field	Description
	• The port is on the master device and no member device is specified.

Related commands

reset igmp-snooping router-port

display igmp-snooping static-group

Use **display igmp-snooping static-group** to display information about static IGMP snooping group entries.

Syntax

In standalone mode:

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]

In IRF mode:

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about static IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about static IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static IGMP snooping group entries for all VLANs.

verbose: Displays detailed information about static IGMP snooping group entries. If you do not specify the keyword, this command displays brief information about static IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static IGMP snooping group entries for the master device. (In IRF mode.)

Examples

Display detailed information about static IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
```

```
Attribute: local port
FSM information: dummy
Host slots (0 in total):
Host ports (1 in total):
  GE1/0/2
```

Table 4 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—No entry exists. • **normal**—The entry is a correct entry.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display igmp-snooping static-router-port

Use **display igmp-snooping static-router-port** to display static router port information.

Syntax

In standalone mode:

display igmp-snooping static-router-port [**vlan** *vlan-id*]

In IRF mode:

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device. (In IRF mode.)

Examples

Display information about static router ports for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 5 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

display igmp-snooping statistics

Use **display igmp-snooping statistics** to display statistics for the IGMP messages learned through IGMP snooping.

Syntax

display igmp-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the IGMP messages learned through 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 PIMv2 hello:  0
Received error IGMP messages:  19
```

Table 6 Command output

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
PIMv2 hello	This field is not supported in the current software version. Number of PIMv2 hello messages.
error IGMP messages	Number of IGMP messages with errors.

Related commands

reset igmp-snooping statistics

display l2-multicast fast-forwarding cache

Use **display l2-multicast fast-forwarding cache** to display Layer 2 multicast fast forwarding entries.

Syntax

In standalone mode:

display l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*source-address* | *group-address*] *

In IRF mode:

display l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*source-address* | *group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command displays Layer 2 multicast fast forwarding entries for all multicast sources.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays Layer 2 multicast fast forwarding entries for all multicast groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast fast forwarding entries for the master device. (In IRF mode.)

Examples

Display Layer 2 multicast fast forwarding entries.

```
<Sysname> display l2-multicast fast-forwarding cache
Total 1 entries, 1 matched

(10.1.1.2,225.1.1.1)
     Status      : Enable                VLAN            : 1
     Source port : 9876                  Destination port: 5432
     Protocol    : 17                    Flag            : 0x2
     Ingress port: GigabitEthernet1/0/2
     List of 1 egress ports:
         GigabitEthernet1/0/1
         Status: Enable                Flag: 0x10
```

Table 7 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 multicast fast forwarding table, and the total number of matching entries.
(10.1.1.2, 225.1.1.1)	(S, G) entry in the Layer 2 multicast fast forwarding table.
Protocol	Protocol number.
VLAN	VLAN ID.
Flag	Flag for the (S, G) entry or the outgoing port. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The port is added to the entry because of packets passed through between cards. • **0x2**—The port is added to an existing entry. • **0x10**—The port is associated with the entry. • **0x20**—The port is to be deleted.
Status	Status of the (S, G) entry or the outgoing port: • **Enabled**—Available. • **Disabled**—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	Outgoing port list of the (S, G) entry.

Related commands

reset l2-multicast fast-forwarding cache all

display l2-multicast ip

Use **display l2-multicast ip** to display information about Layer 2 IP multicast groups.

Syntax

In standalone mode:

display l2-multicast ip [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]

In IRF mode:

display l2-multicast ip [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays information about all Layer 2 IP multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about Layer 2 IP multicast groups for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IP multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device. (In IRF mode.)

Examples

Display information about Layer 2 IP multicast groups for VLAN 2.

```
<Sysname> display l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/1                              (S, SUC)
```

Table 8 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.

Field	Description
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast groups in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by PIM. PIM is not supported in the current software version. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—PIM port. PIM is not supported in the current software version. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing has succeeded. • **F**—Processing has failed. • **BC**—In a VLAN, the port is a TRILL port that floods multicast data after the topology changes. TRILL is not supported in the current software version.

display l2-multicast ip forwarding

Use **display l2-multicast ip forwarding** to display Layer 2 multicast IP forwarding entries.

Syntax

In standalone mode:

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]

In IRF mode:

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays Layer 2 multicast IP forwarding entries for all multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays Layer 2 multicast IP forwarding entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast IP forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast IP forwarding entries for the master device. (In IRF mode.)

Examples

Display Layer 2 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (1 in total):
      GigabitEthernet1/0/1
```

Table 9 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast IP forwarding entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 multicast IP forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host ports (1 in total)	Member ports and total number of member ports.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.

display l2-multicast mac

Use **display l2-multicast mac** to display information about Layer 2 MAC multicast groups.

Syntax

In standalone mode:

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*]

In IRF mode:

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its multicast MAC address. If you do not specify a MAC multicast group, this command displays information about all Layer 2 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 MAC multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 MAC multicast groups for the master device. (In IRF mode.)

Examples

Display information about Layer 2 MAC multicast groups for VLAN 2.

```
<Sysname> display l2-multicast mac vlan 2
Total 1 MAC entries.

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/1
```

Table 10 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
MAC group address	Address of the MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display l2-multicast mac forwarding

Use **display l2-multicast mac forwarding** to display Layer 2 multicast MAC forwarding entries.

Syntax

In standalone mode:

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*]

In IRF mode:

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this command displays Layer 2 multicast MAC forwarding entries for all MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast MAC forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast MAC group entries for the master device. (In IRF mode.)

Examples

Display Layer 2 multicast MAC forwarding entries for VLAN 2.

```
<Sysname> display l2-multicast mac forwarding vlan 2
Total 1 MAC entries.

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Host slots (0 in total):
    Host ports (1 in total):
      GigabitEthernet1/0/1
```

Table 11 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 multicast MAC forwarding entries.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the MAC multicast group.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

dot1p-priority (IGMP-snooping view)

Use **dot1p-priority** to set the 802.1p priority for IGMP messages globally.

Use **undo dot1p-priority** to restore the default.

Syntax

dot1p-priority *priority*

undo dot1p-priority

Default

The 802.1p priority is not set for IGMP messages.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for IGMP messages to 3 globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

Related commands

igmp-snooping dot1p-priority

drop-unknown (IGMP-snooping view)

Use **drop-unknown** to enable dropping unknown multicast data packets globally.

Use **undo drop-unknown** to disable dropping unknown multicast data packets globally.

Syntax

drop-unknown

undo drop-unknown

Default

Dropping unknown multicast data packets is disabled, and unknown multicast data packets are flooded.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view.

The **igmp-snooping drop-unknown** command and the **drop-unknown** command in IGMP-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

Enable dropping unknown multicast data packets globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] drop-unknown
```

Related commands

igmp-snooping drop-unknown

enable (IGMP-snooping view)

Use **enable** to enable IGMP snooping for VLANs.

Use **undo enable** to disable IGMP snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

IGMP snooping is disabled in a VLAN.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for VLANs.

You can enable IGMP snooping for multiple VLANs by using this command in IGMP-snooping view or for a VLAN by using the **igmp-snooping enable** command in VLAN view. The configuration in IGMP-snooping view has the same priority as the configuration in VLAN view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2 through VLAN 10.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
```

Related commands

igmp-snooping

igmp-snooping enable

entry-limit (IGMP-snooping view)

Use **entry-limit** to globally set the maximum number of IGMP snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of IGMP snooping forwarding entries is 4294967295.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IGMP snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of IGMP snooping forwarding entries to 512.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] entry-limit 512
```

fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable fast-leave processing for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

Related commands

igmp-snooping fast-leave

group-policy (IGMP-snooping view)

Use **group-policy** to globally configure a multicast group policy to control the multicast groups that hosts can join.

Use **undo group-policy** to globally delete multicast group policies.

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No multicast group policies exist. Hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

Related commands

igmp-snooping group-policy

host-aging-time (IGMP-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

Related commands

igmp-snooping host-aging-time

igmp-snooping

Use **igmp-snooping** to enable the IGMP snooping feature and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable the IGMP snooping feature.

Syntax

igmp-snooping

undo igmp-snooping

Default

The IGMP snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the IGMP snooping feature, IGMP snooping is disabled in all VLANs.

Examples

Enable the IGMP snooping feature and enter IGMP-snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping dot1p-priority

Use **igmp-snooping dot1p-priority** to set the 802.1p priority for IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

Default

The 802.1p priority is not set for IGMP messages.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. The VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the 802.1p priority for IGMP messages to 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping dot1p-priority 3
```

Related commands

dot1p-priority (IGMP-snooping view)

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping drop-unknown

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data packets for a VLAN.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data packets for a VLAN.

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

Dropping unknown multicast data packets is disabled. Unknown multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can enable this feature for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view.

The **igmp-snooping drop-unknown** command and the **drop-unknown** command in IGMP-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

In VLAN 2, enable IGMP snooping, and enable dropping unknown multicast data packets.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

Related commands

drop-unknown (IGMP-snooping view)

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping enable

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN.

Use **undo igmp-snooping enable** to disable IGMP snooping in a VLAN.

Syntax

igmp-snooping enable

undo igmp-snooping enable

Default

IGMP snooping is disabled in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for a VLAN.

You can enable IGMP snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command in IGMP-snooping view. The configuration in VLAN view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping

igmp-snooping fast-leave

Use **igmp-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

Related commands

fast-leave (IGMP-snooping view)

igmp-snooping general-query source-ip

Use **igmp-snooping general-query source-ip** to configure the source IP address for IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

Default

In a VLAN, the source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP general queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

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] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping group-limit

Use **igmp-snooping group-limit** to set the maximum number of multicast groups that a port can join.

Use **undo igmp-snooping group-limit** to remove the limit on the maximum number of multicast groups that a port can join.

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number of multicast groups the port can join in VLAN 2 to 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Use **igmp-snooping group-policy** to configure a multicast group policy on a port to control the multicast groups that hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to delete multicast group policies on a port.

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

Default

No multicast group polices exist on a port. Hosts attached to the port can join any multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs on a port for different VLANs. If you configure multiple ACLs on a port for the same VLAN, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (IGMP-snooping view)

igmp-snooping host-aging-time

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN.

Use **undo igmp-snooping host-aging-time** to restore the default.

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic member ports to 300 seconds.

```
<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
```

Related commands

enable (IGMP-snooping view)

host-aging-time (IGMP-snooping view)

igmp-snooping enable

igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the configuration of a simulated member host for a multicast group.

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* | **all** }

Default

A port is not configured as a simulated member host for multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, this command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Usage guidelines

The version of IGMP running on a simulated member host is the same as the version of IGMP snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host of the multicast source and group (1.1.1.1, 232.1.1.1) 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 version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan
2
```

igmp-snooping last-member-query-interval

Use **igmp-snooping last-member-query-interval** to set the IGMP last member query interval for a VLAN.

Use **undo igmp-snooping last-member-query-interval** to restore the default.

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```
<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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

last-member-query-interval (IGMP-snooping view)

igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure the source IP address for IGMP leave messages.

Use **undo igmp-snooping leave source-ip** to restore the default.

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

Default

In a VLAN, the source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP leave messages.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP leave messages.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping max-response-time

Use **igmp-snooping max-response-time** to set the maximum response time for IGMP general queries in a VLAN.

Use **undo igmp-snooping max-response-time** to restore the default.

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

In VLAN 2, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.

```
<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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping query-interval

max-response-time (IGMP-snooping view)

igmp-snooping overflow-replace

Use **igmp-snooping overflow-replace** to enable multicast group replacement on a port.

Use **undo igmp-snooping overflow-replace** to disable multicast group replacement on a port.

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

Default

Multicast group replacement is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable multicast group replacement for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable multicast group replacement for VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping view)

igmp-snooping querier

Use **igmp-snooping querier** to enable the IGMP snooping querier.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier.

Syntax

igmp-snooping querier

undo igmp-snooping querier

Default

The IGMP snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN.

Use **undo igmp-snooping query-interval** to restore the default.

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

Default

The IGMP general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 2 to 31744 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

To avoid mistakenly deleting multicast group members, set the IGMP general query interval to be greater than the maximum response time for IGMP general queries.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.

```
<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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping max-response-time

igmp-snooping querier

max-response-time

igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure the source IP address for IGMP reports.

Use **undo igmp-snooping report source-ip** to restore the default.

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

Default

In a VLAN, the source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP reports.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP reports.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping router-aging-time

Use **igmp-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN.

Use **undo igmp-snooping router-aging-time** to restore the default.

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic router ports to 100 seconds.

```
<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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

router-aging-time (IGMP-snooping view)

igmp-snooping router-port-deny

Use **igmp-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo igmp-snooping router-port-deny** to allow a port to become a dynamic router port.

Syntax

igmp-snooping router-port-deny [**vlan** *vlan-list*]

undo igmp-snooping router-port-deny [**vlan** *vlan-list*]

Default

A port is allowed to become a dynamic router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, this command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, this command takes effect on all VLANs to which the port belongs.

Examples

Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping router-port-deny vlan 2
```

igmp-snooping special-query source-ip

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

Use **undo igmp-snooping special-query source-ip** to restore the default.

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

Default

In a VLAN, the source IP address of IGMP group-specific queries is one of the following:

- The source address of IGMP group-specific queries if the IGMP snooping querier of the VLAN has received IGMP general queries.
- The IP address of the current VLAN interface if the IGMP snooping querier does not receive an IGMP general query.
- 0.0.0.0 if the IGMP snooping querier does not receive an IGMP general query and the current VLAN interface does not have an IP address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP group-specific queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

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] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static member port of a multicast group.

Use **undo igmp-snooping static-group** to remove the configuration of static member ports.

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* | **all** }

Default

A port is not a static member port of a multicast group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a static member port for a multicast source and group. If you do not specify a multicast source, this command configures the port as a static member port for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port of the multicast source and group (1.1.1.1, 225.0.0.1) 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 version 3
[Sysname-vlan2] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1
vlan 2
```

igmp-snooping static-router-port

Use **igmp-snooping static-router-port** to configure a port as a static router port.

Use **undo igmp-snooping static-router-port** to remove the configuration of static router ports.

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

`all`: Specifies all VLANs.

`vlan` *`vlan-id`*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Use **`igmp-snooping version`** to specify an IGMP snooping version for a VLAN.

Use **`undo igmp-snooping version`** to restore the default.

Syntax

`igmp-snooping version` *`version-number`*

`undo igmp-snooping version`

Default

The IGMP snooping version in a VLAN is 2.

Views

VLAN view

Predefined user roles

network-admin

Parameters

`version-number`: Specifies an IGMP snooping version, 2 or 3.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. The VLAN-specific configuration has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable IGMP snooping, and specify IGMP snooping 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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

version (IGMP-snooping view)

last-member-query-interval (IGMP-snooping view)

Use **last-member-query-interval** to set the IGMP last member query interval globally.

Use **undo last-member-query-interval** to restore the default.

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

Related commands

igmp-snooping last-member-query-interval

max-response-time (IGMP-snooping view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

Set the global maximum response time for IGMP general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

Related commands

igmp-snooping max-response-time

igmp-snooping query-interval

overflow-replace (IGMP-snooping view)

Use **overflow-replace** to enable the multicast group replacement feature globally.

Use **undo overflow-replace** to disable the multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The multicast group replacement feature is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable the multicast group replacement feature globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

Related commands

igmp-snooping overflow-replace

report-aggregation (IGMP-snooping view)

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

IGMP report suppression is enabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Examples

Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Use **reset igmp-snooping group** to clear information about dynamic IGMP snooping group entries.

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears information about dynamic IGMP snooping group entries for all multicast sources.

all: Specifies all multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic IGMP snooping group entries for all VLANs.

Examples

Clear information about all dynamic IGMP snooping group entries.

```
<Sysname> reset igmp-snooping group all
```

Related commands

display igmp-snooping group

reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to clear dynamic router port information.

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

Examples

Clear dynamic router port information.

```
<Sysname> reset igmp-snooping router-port all
```

Related commands

display igmp-snooping router-port

reset igmp-snooping statistics

Use **reset igmp-snooping statistics** to clear statistics for IGMP messages learned through IGMP snooping.

Syntax

reset igmp-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the statistics for all IGMP messages learned through IGMP snooping.

```
<Sysname> reset igmp-snooping statistics
```

Related commands

display igmp-snooping statistics

reset l2-multicast fast-forwarding cache

Use **reset l2-multicast fast-forwarding cache** to clear Layer 2 multicast fast forwarding entries.

Syntax

In standalone mode:

reset l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *source-address* | *group-address* } * | **all** }

In IRF mode:

reset l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

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.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears Layer 2 multicast fast forwarding entries for the master device. (In IRF mode.)

all: Specifies all Layer 2 multicast fast forwarding entries.

Examples

Clear all Layer 2 multicast fast forwarding entries.

```
<Sysname> reset l2-multicast fast-forwarding cache all
```

Clear the Layer 2 multicast fast forwarding entry for the multicast source and group (20.0.0.2, 225.0.0.2).

```
<Sysname> reset l2-multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

Related commands

display l2-multicast fast-forwarding cache

router-aging-time (IGMP-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

Related commands

igmp-snooping router-aging-time

version (IGMP-snooping view)

Use **version** to specify an IGMP snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The IGMP snooping version in a VLAN is 2.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable IGMP snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in IGMP-snooping view or for a VLAN in VLAN view. The configuration in IGMP-snooping view has the same priority as the VLAN-specific configuration, and the most recent configuration takes effect.

Examples

Enable IGMP snooping for VLAN 2 through VLAN 10, and specify IGMP snooping version 3 for these VLANs.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
[Sysname-igmp-snooping] version 3 vlan 2 to 10
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping version

Contents

MLD snooping commands 1

display ipv6 l2-multicast fast-forwarding cache 2
display ipv6 l2-multicast ip 3
display ipv6 l2-multicast ip forwarding 5
display ipv6 l2-multicast mac 6
display ipv6 l2-multicast mac forwarding 7
display mld-snooping 8
display mld-snooping group 10
display mld-snooping router-port 12
display mld-snooping static-group 13
display mld-snooping static-router-port 15
display mld-snooping statistics 16
dot1p-priority (MLD-snooping view) 17
drop-unknown (MLD-snooping view) 17
enable (MLD-snooping view) 18
entry-limit (MLD-snooping view) 19
fast-leave (MLD-snooping view) 19
group-policy (MLD-snooping view) 20
host-aging-time (MLD-snooping view) 21
last-listener-query-interval (MLD-snooping view) 22
max-response-time (MLD-snooping view) 23
mld-snooping 24
mld-snooping done source-ip 24
mld-snooping dot1p-priority 25
mld-snooping drop-unknown 26
mld-snooping enable 27
mld-snooping fast-leave 27
mld-snooping general-query source-ip 28
mld-snooping group-limit 29
mld-snooping group-policy 30
mld-snooping host-aging-time 31
mld-snooping host-join 32
mld-snooping last-listener-query-interval 33
mld-snooping max-response-time 34
mld-snooping overflow-replace 35
mld-snooping querier 35
mld-snooping query-interval 36
mld-snooping report source-ip 37
mld-snooping router-aging-time 38
mld-snooping router-port-deny 38
mld-snooping special-query source-ip 39
mld-snooping static-group 40
mld-snooping static-router-port 41
mld-snooping version 41
overflow-replace (MLD-snooping view) 42
report-aggregation (MLD-snooping view) 43
reset ipv6 l2-multicast fast-forwarding cache 43
reset mld-snooping group 44
reset mld-snooping router-port 45
reset mld-snooping statistics 45
router-aging-time (MLD-snooping view) 46
version (MLD-snooping view) 46

MLD snooping commands

The following compatibility matrixes show the support of hardware platforms for MLD snooping:

Hardware series	Model	Product code	MLD snooping compatibility
WX1800H series	WX1804H-PWR	EWP-WX1804H-PWR-CN	Yes
WX2500H series	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
MAK series	MAK204 MAK206	EWP-MAK204 EWP-MAK206	Yes
WX3000H series	WX3010H WX3010H-X-PWR WX3010H-L WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X • WX3024H • WX3024H-F No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	Yes
WX5500E series	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Yes

Hardware series	Model	Product code	MLD snooping compatibility
WX1800H series	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800H series	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800H series	WX5860H	EWP-WX5860H-GL	Yes

The WX1800H series, WX2500H series, MAK series, and WX3000H series access controllers do not support parameters or commands that are available only in IRF mode.

display ipv6 l2-multicast fast-forwarding cache

Use **display ipv6 l2-multicast fast-forwarding cache** to display Layer 2 IPv6 multicast fast forwarding entries.

Syntax

In standalone mode:

display ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*ipv6-source-address* | *ipv6-group-address*] *

In IRF mode:

display ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*ipv6-source-address* | *ipv6-group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 multicast sources.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 multicast groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast fast forwarding entries for the master device. (In IRF mode.)

Examples

Display Layer 2 IPv6 multicast fast forwarding entries.

```
<Sysname> display ipv6 l2-multicast fast-forwarding cache
```

```
Total 1 entries, 1 matched

(1::6, FF1E::2)
      Status      : Enable                VLAN            : 1
      Source port : 9876                  Destination port: 5432
      Protocol    : 17                    Flag            : 0x2
      Ingress port: GigabitEthernet1/0/2
      List of 1 egress ports:
           GigabitEthernet1/0/1
           Status: Enable               Flag: 0x10
```

Table 1 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 IPv6 multicast fast forwarding table, and the total number of matching entries.
(1::6, FF1E::2)	(S, G) entry in the Layer 2 IPv6 multicast fast forwarding table.
Protocol	Protocol number.
VLAN	VLAN ID.
Flag	Flag for the (S, G) entry or the outgoing port. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The port is added to the entry because of packets passed through between cards. • **0x2**—The port is added to an existing entry. • **0x10**—The port is associated with the entry. • **0x20**—The port is to be deleted.
Status	Status of the (S, G) entry or the outgoing port: • **Enabled**—Available. • **Disabled**—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	List of outgoing ports of the (S, G) entry.

Related commands

`reset ipv6 l2-multicast fast-forwarding cache all`

display ipv6 l2-multicast ip

Use **`display ipv6 l2-multicast ip`** to display information about Layer 2 IPv6 multicast groups.

Syntax

In standalone mode:

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*]

In IRF mode:

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays information about all Layer 2 IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about Layer 2 IPv6 multicast groups for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device. (In IRF mode.)

Examples

Display information about Layer 2 IPv6 multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 IP entries.
   (::, FF1E::101)
    Attribute: static, success
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/1                              (S, SUC)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast groups.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IPv6 multicast groups in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by IPv6 PIM. IPv6 PIM is not supported in the

Field	Description
	current software version. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—IPv6 PIM port. IPv6 PIM is not supported in the current software version. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing has succeeded. • **F**—Processing has failed. • **BC**—In a VLAN, the port is a TRILL port that floods IPv6 multicast data after the topology changes. TRILL is not supported in the current software version.

display ipv6 l2-multicast ip forwarding

Use **display ipv6 l2-multicast ip forwarding** to display Layer 2 IPv6 multicast IP forwarding entries.

Syntax

In standalone mode:

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*]

In IRF mode:

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast IP forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast IP forwarding entries for the master device. (In IRF mode.)

Examples

Display Layer 2 IPv6 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 IP entries.
   (::, FF1E::101)
    Host slots (0 in total):
    Host ports (1 in total):
      GigabitEthernet1/0/1
```

Table 3 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IPv6 multicast IP forwarding entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac

Use **display ipv6 l2-multicast mac** to display information about Layer 2 IPv6 multicast MAC multicast groups.

Syntax

In standalone mode:

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id*]

In IRF mode:

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 multicast MAC address. If you do not specify an IPv6 multicast MAC address, this command displays information about all Layer 2 IPv6 multicast MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for the master device. (In IRF mode.)

Examples

Display information about Layer 2 IPv6 multicast MAC multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac vlan 2
Total 1 MAC entries.

VLAN 2: Total 1 MAC entries.
  MAC group address: 3333-0000-0101
    Attribute: success
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/1
```

Table 4 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 IPv6 MAC multicast groups in VLAN 2.
MAC group address	IPv6 address of the Layer 2 IPv6 MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac forwarding

Use **display ipv6 l2-multicast mac forwarding** to display Layer 2 IPv6 multicast MAC forwarding entries.

Syntax

In standalone mode:

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*]

In IRF mode:

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all IPv6 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast MAC forwarding entries for the master device. (In IRF mode.)

Examples

Display Layer 2 IPv6 multicast MAC forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac forwarding vlan 2
Total 1 MAC entries.

VLAN 2: Total 1 MAC entries.
  MAC group address: 3333-0000-0101
    Host slots (0 in total):
    Host ports (1 in total):
      GigabitEthernet1/0/1
```

Table 5 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the IPv6 MAC multicast group.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports, and the total number of member ports.

display mld-snooping

Use **display mld-snooping** to display MLD snooping status.

Syntax

display mld-snooping [**global** | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global MLD snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays the global MLD snooping status and the MLD snooping status in all VLANs.

Examples

Display the global MLD snooping status and the MLD snooping status for all VLANs.

```
<Sysname> display mld-snooping
MLD snooping information: Global
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Report-aggregation: Enabled
 Dot1p-priority: --

MLD snooping information: VLAN 1
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Enabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Dot1p-priority: 2

MLD snooping information: VLAN 10
 MLD snooping: Enabled
 Drop-unknown: Enabled
```

```
Version: 1
Host-aging-time: 260s
Router-aging-time: 260s
Max-response-time: 10s
Last-listener-query-interval: 1s
Querier: Enabled
Query-interval: 125s
General-query source IP: FE80::2FF:FFFF:FE00:1
Special-query source IP: FE80::2FF:FFFF:FE00:1
Report source IP: FE80::2FF:FFFF:FE00:2
Done source IP: FE80::2FF:FFFF:FE00:3
Dot1p-priority: --
```

Table 6 Command output

Field	Description
MLD snooping	MLD snooping status in a VLAN: • Enabled. • Disabled.
Drop-unknown	Status of dropping unknown IPv6 multicast data: • Enabled. • Disabled.
Version	MLD snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum time for responding to MLD general queries.
Last-listener-query-interval	Interval for sending MLD multicast-address-specific queries.
Report-aggregation	Status of MLD report suppression: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for MLD messages. This field displays two hyphens (--) if the 802.1p priority is not configured.
Querier	Status of MLD snooping querier: • Enabled. • Disabled.
Query-interval	Interval for sending MLD general queries.
General-query source IP	Source IPv6 address of MLD general queries.
Special-query source IP	Source IPv6 address of MLD multicast-address-specific queries.
Report source IP	Source IPv6 address of MLD reports.
Done source IP	Source IPv6 address of MLD done messages.

display mld-snooping group

Use **display mld-snooping group** to display information about dynamic MLD snooping group entries.

Syntax

In standalone mode:

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**]

In IRF mode:

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all dynamic MLD snooping group entries.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about dynamic MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic MLD snooping group entries for all VLANs.

verbose: Displays detailed information about dynamic MLD snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic MLD snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic MLD snooping group entries for the master device. (In IRF mode.)

Examples

Display detailed information about dynamic MLD snooping group entries for VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                             (00:03:23)
```

Table 7 Command output

Field	Description
Total 1 entries	Total number of dynamic MLD snooping group entries.

Field	Description
VLAN 2: Total 1 entries	Total number of dynamic MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.
(00:03:23)	Remaining aging time for the dynamic member port. This field is always displayed for a global port. (In standalone mode.) For a non-global port, this field is always displayed. (In IRF mode.) For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

`reset mld-snooping group`

display mld-snooping router-port

Use **`display mld-snooping router-port`** to display dynamic router port information.

Syntax

In standalone mode:

`display mld-snooping router-port` [**`verbose`** | **`vlan`** *`vlan-id`*] [**`verbose`**]

In IRF mode:

`display mld-snooping router-port` [**`verbose`** | **`vlan`** *`vlan-id`*] [**`verbose`**] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about dynamic router ports. If you do not specify this keyword, the command displays brief information about dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device. (In IRF mode.)

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Sysname> display mld-snooping router-port vlan 2
VLAN 2:
  Router ports (1 in total):
    WLAN-BSS1/0/10                          (00:01:30)
```

Table 8 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (1 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. This field is always displayed for a global port (including Layer 2 aggregate interfaces). (In standalone mode.) For a non-global port, this field is always displayed. (In IRF mode.) For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset mld-snooping router-port

display mld-snooping static-group

Use **display mld-snooping static-group** to display information about static MLD snooping group entries.

Syntax

In standalone mode:

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**]

In IRF mode:

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about static MLD snooping group entries for all IPv6 multicast groups.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about static MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static MLD snooping group entries for all VLANs.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static MLD snooping group entries for the master device. (In IRF mode.)

Examples

Display detailed information about static MLD snooping group entries for VLAN 2.

```
<Sysname> display mld-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 9 Command output

Field	Description
Total 1 entries	Total number of static MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of static MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed.

Field	Description
	• **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Host slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display mld-snooping static-router-port

Use **display mld-snooping static-router-port** to display static router port information.

Syntax

In standalone mode:

display mld-snooping static-router-port [**vlan** *vlan-id*]

In IRF mode:

display mld-snooping static-router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device. (In IRF mode.)

Examples

Display information about static router ports for VLAN 2.

```
<Sysname> display mld-snooping static-router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 10 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	(In standalone mode.) This field is not supported. (In IRF mode.) Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

display mld-snooping statistics

Use **display mld-snooping statistics** to display statistics for the MLD messages learned through MLD snooping.

Syntax

display mld-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the MLD messages learned through 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 IPv6 PIM hello:  0
Received error MLD messages:  0
```

Table 11 Command output

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
dones	Number of MLD done messages.

Field	Description
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.
IPv6 PIM hello	This field is not supported in the current software version. Number of IPv6 PIM hello messages.
error MLD messages	Number of MLD messages with errors.

Related commands

`reset mld-snooping statistics`

dot1p-priority (MLD-snooping view)

Use **`dot1p-priority`** to set the 802.1p priority for MLD messages globally.

Use **`undo dot1p-priority`** to restore the default.

Syntax

`dot1p-priority` *`priority`*

`undo dot1p-priority`

Default

The 802.1p priority is not set for MLD messages.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

`priority`: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for MLD messages to 3 globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dot1p-priority 3
```

Related commands

`mld-snooping dot1p-priority`

drop-unknown (MLD-snooping view)

Use **`drop-unknown`** to enable dropping unknown IPv6 multicast data packets globally.

Use **`undo drop-unknown`** to disable dropping unknown IPv6 multicast data packets globally.

Syntax

drop-unknown

undo drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled, and unknown IPv6 multicast data packets are flooded.

Views

MLD-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view.

The **mld-snooping drop-unknown** command and the **drop-unknown** command in MLD-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

Enable dropping unknown IPv6 multicast data packets globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] drop-unknown
```

Related commands

mld-snooping drop-unknown

enable (MLD-snooping view)

Use **enable** to enable MLD snooping for VLANs.

Use **undo enable** to disable MLD snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

MLD snooping is disabled in a VLAN.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for VLANs.

You can enable MLD snooping for multiple VLANs by using this command in MLD-snooping view or for a VLAN by using the **mld-snooping enable** command in VLAN view. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2 through VLAN 10.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
```

Related commands

mld-snooping

mld-snooping enable

entry-limit (MLD-snooping view)

Use **entry-limit** to globally set the maximum number of MLD snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of MLD snooping forwarding entries is 4294967295.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of MLD snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of MLD snooping forwarding entries to 512.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] entry-limit 512
```

fast-leave (MLD-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable MLD snooping fast-leave processing for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

Related commands

mld-snooping fast-leave

group-policy (MLD-snooping view)

Use **group-policy** to globally configure an IPv6 multicast group policy to control the IPv6 multicast groups that hosts can join.

Use **undo group-policy** to globally delete IPv6 multicast group policies.

Syntax

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts can join any IPv6 multicast groups.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports, set the **source** *source-address source-prefix* option to 0::0.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

Related commands

mld-snooping group-policy

host-aging-time (MLD-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

Related commands

mld-snooping host-aging-time

last-listener-query-interval (MLD-snooping view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

Related commands

mld-snooping last-listener-query-interval

max-response-time (MLD-snooping view)

Use **max-response-time** to set the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

Set the global maximum response time for MLD general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

Related commands

mld-snooping max-response-time

mld-snooping query-interval

mld-snooping

Use **mld-snooping** to enable the MLD snooping feature and enter MLD-snooping view.

Use **undo mld-snooping** to disable the MLD snooping feature.

Syntax

mld-snooping

undo mld-snooping

Default

The MLD snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the MLD snooping feature, MLD snooping is disabled in all VLANs.

Examples

Enable the MLD snooping feature and enter MLD-snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping done source-ip

Use **mld-snooping done source-ip** to configure the source IPv6 address for MLD done messages.

Use **undo mld-snooping done source-ip** to restore the default.

Syntax

mld-snooping done source-ip *ipv6-address*

undo mld-snooping done source-ip

Default

In a VLAN, the source IPv6 address of MLD done messages is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD done messages.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD done messages.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping done source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping dot1p-priority

Use **mld-snooping dot1p-priority** to set the 802.1p priority for MLD messages in a VLAN.

Use **undo mld-snooping dot1p-priority** to restore the default.

Syntax

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

Default

The 802.1p priority is not set for MLD messages.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the 802.1p priority for MLD messages to 3.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
```

```
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping dot1p-priority 3
```

Related commands

dot1p-priority (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

mld-snooping drop-unknown

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data packets for a VLAN.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data packets for a VLAN.

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled. Unknown IPv6 multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can enable this feature for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view.

The **mld-snooping drop-unknown** command and the **drop-unknown** command in MLD-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

In VLAN 2, enable MLD snooping, and enable dropping unknown IPv6 multicast data packets.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

Related commands

drop-unknown (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

mld-snooping enable

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **undo mld-snooping enable** to disable MLD snooping for a VLAN.

Syntax

mld-snooping enable

undo mld-snooping enable

Default

MLD snooping is disabled in a VLAN

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for a VLAN.

You can enable MLD snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

Related commands

enable (MLD-snooping view)

mld-snooping

mld-snooping fast-leave

Use **mld-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

Related commands

fast-leave (MLD-snooping view)

mld-snooping general-query source-ip

Use **mld-snooping general-query source-ip** to configure the source IPv6 address for MLD general queries.

Use **undo mld-snooping general-query source-ip** to restore the default.

Syntax

mld-snooping general-query source-ip *ipv6-address*

undo mld-snooping general-query source-ip

Default

In a VLAN, the source IPv6 address for MLD general queries is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD general queries.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD general queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping group-limit

Use **mld-snooping group-limit** to set the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to remove the limit on the maximum number of IPv6 multicast groups that a port can join.

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of IPv6 multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number to 10 for IPv6 multicast groups that the port can join in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Use **mld-snooping group-policy** to configure an IPv6 multicast group policy on a port to control the IPv6 multicast groups that hosts attached to the port can join.

Use **undo mld-snooping group-policy** to delete IPv6 multicast group policies on a port.

Syntax

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts attached to the port can join any IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999. Hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports and MLD IS_EX and MLDv2 TO_EX reports that do not carry IPv6 multicast source addresses, set the **source** *source-address source-prefix* option to 0::0.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for different VLANs on a port. If you configure multiple ACLs for the same VLANs on a port, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 multicast group policy for VLAN 2 so that hosts attached to the port in VLAN 2 can join only the group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (MLD-snooping view)

mld-snooping host-aging-time

Use **mld-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN.

Use **undo mld-snooping host-aging-time** to restore the default.

Syntax

mld-snooping host-aging-time *seconds*

undo mld-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic member ports in the VLAN to 300 seconds.

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

```
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-aging-time 300
```

Related commands

enable (MLD-snooping view)

host-aging-time (MLD-snooping view)

mld-snooping enable

mld-snooping host-join

Use **mld-snooping host-join** to configure a port as a simulated member host for an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping host-join** to remove the configuration of a simulated member host for an IPv6 multicast group.

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* | **all** }

Default

A port is not a simulated member host of any IPv6 multicast groups or any IPv6 multicast sources and groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Usage guidelines

The version of MLD running on a simulated member host is the same as the version of MLD snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 vlan 2
```

mld-snooping last-listener-query-interval

Use **mld-snooping last-listener-query-interval** to set the MLD last listener query interval for a VLAN.

Use **undo mld-snooping last-listener-query-interval** to restore the default.

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the interval for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the MLD last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

Related commands

enable (MLD-snooping view)

last-listener-query-interval (MLD-snooping view)

mld-snooping enable

mld-snooping max-response-time

Use **mld-snooping max-response-time** to set the maximum response time for MLD general queries in a VLAN.

Use **undo mld-snooping max-response-time** to restore the default.

Syntax

mld-snooping max-response-time *seconds*

undo mld-snooping max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

In VLAN 2, enable MLD snooping, and set the maximum response time for MLD general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping max-response-time 5
```

Related commands

enable (MLD-snooping view)

max-response-time (MLD-snooping view)

mld-snooping enable

mld-snooping query-interval

mld-snooping overflow-replace

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement feature on a port.

Use **undo mld-snooping overflow-replace** to disable the multicast group replacement feature on a port.

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable the IPv6 multicast group replacement feature for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (MLD-snooping view)

mld-snooping querier

Use **mld-snooping querier** to enable the MLD snooping querier.

Use **undo mld-snooping querier** to disable the MLD snooping querier.

Syntax

mld-snooping querier

undo mld-snooping querier

Default

The MLD snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and enable the MLD snooping querier.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

Related commands

`enable` (MLD-snooping view)

`mld-snooping enable`

mld-snooping query-interval

Use **`mld-snooping query-interval`** to set the MLD general query interval for a VLAN.

Use **`undo mld-snooping query-interval`** to restore the default.

Syntax

`mld-snooping query-interval` *`interval`*

`undo mld-snooping query-interval`

Default

The MLD general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

`interval`: Specifies an MLD general query interval, in the range of 2 to 31744 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

Examples

In VLAN 2, enable MLD snooping, and set the MLD general query interval to 20 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping query-interval 20
```

Related commands

enable (MLD-snooping view)

max-response-time

mld-snooping enable

mld-snooping max-response-time

mld-snooping querier

mld-snooping report source-ip

Use **mld-snooping report source-ip** to configure the source IPv6 address for MLD reports.

Use **undo mld-snooping report source-ip** to restore the default.

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

Default

In a VLAN, the source IPv6 address for MLD reports is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD reports.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD reports.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping report source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping router-aging-time

Use **mld-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN.

Use **undo mld-snooping router-aging-time** to restore the default.

Syntax

mld-snooping router-aging-time *seconds*

undo mld-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic router ports in the VLAN to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping router-aging-time 100
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

router-aging-time (MLD-snooping view)

mld-snooping router-port-deny

Use **mld-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo mld-snooping router-port-deny** to allow a port to become a dynamic router port.

Syntax

mld-snooping router-port-deny [**vlan** *vlan-list*]

undo mld-snooping router-port-deny [**vlan** *vlan-list*]

Default

A port is allowed to become a dynamic router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, this command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, this command takes effect on all VLANs.

Examples

Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping router-port-deny vlan 2
```

mld-snooping special-query source-ip

Use **mld-snooping special-query source-ip** to configure the source IPv6 address for MLD multicast-address-specific queries.

Use **undo mld-snooping special-query source-ip** to restore the default.

Syntax

mld-snooping special-query source-ip *ipv6-address*

undo mld-snooping special-query source-ip

Default

In a VLAN, the source IPv6 address of MLD multicast-address-specific queries is one of the following:

- The source address of MLD general queries if the MLD snooping querier of the VLAN has received MLD general queries.
- The IPv6 link-local address of the current VLAN interface if the MLD snooping querier does not receive an MLD general query.
- FE80::02FF:FFFF:FE00:0001 if the MLD snooping querier does not receive an MLD general query and the current VLAN interface does not have an IPv6 link-local address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD multicast-address-specific queries.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping static-group

Use **mld-snooping static-group** to configure a port as a static member port of an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping static-group** to delete the configuration of static member ports.

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* | **all** }

Default

A port is not a static member port of IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 vlan 2
```

mld-snooping static-router-port

Use **mld-snooping static-router-port** to configure a port as a static router port.

Use **undo mld-snooping static-router-port** to remove the configuration of static router ports.

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2
```

mld-snooping version

Use **mld-snooping version** to specify an MLD snooping version for a VLAN.

Use **undo mld-snooping version** to restore the default.

Syntax

mld-snooping version *version-number*

undo mld-snooping version

Default

The MLD snooping version in a VLAN is 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

Usage guidelines

You must enable MLD snooping for a VLAN before you configure this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in MLD-snooping view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable MLD snooping, and specify MLD snooping 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
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

version (MLD-snooping view)

overflow-replace (MLD-snooping view)

Use **overflow-replace** to enable the IPv6 multicast group replacement feature globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable IPv6 multicast group replacement globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

Related commands

mld-snooping overflow-replace

report-aggregation (MLD-snooping view)

Use **report-aggregation** to enable MLD report suppression.

Use **undo report-aggregation** to disable MLD report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

MLD report suppression is enabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Examples

Disable MLD report suppression.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

reset ipv6 l2-multicast fast-forwarding cache

Use **reset ipv6 l2-multicast fast-forwarding cache** to clear Layer 2 IPv6 multicast fast forwarding entries.

Syntax

In standalone mode:

reset ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *ipv6-source-address* | *ipv6-group-address* } * | **all** }

In IRF mode:

reset ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears Layer 2 IPv6 multicast fast forwarding entries for the master device. (In IRF mode.)

all: Specifies all Layer 2 IPv6 multicast fast forwarding entries.

Examples

Clear all Layer 2 IPv6 multicast fast forwarding entries.

```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache all
```

Clear the Layer 2 IPv6 multicast fast forwarding entry for the IPv6 group (*, FF1E::2).

```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache FF1E::2
```

Related commands

display ipv6 l2-multicast fast-forwarding cache

reset mld-snooping group

Use **reset mld-snooping group** to clear information about dynamic MLD snooping group entries.

Syntax

reset mld-snooping group { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command clears information about dynamic MLD snooping group entries for all IPv6 multicast sources.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic MLD snooping group entries for all VLANs.

Examples

Clear information about all dynamic MLD snooping group entries.

```
<Sysname> reset mld-snooping group all
```

Related commands

display mld-snooping group

reset mld-snooping router-port

Use **reset mld-snooping router-port** to clear dynamic router port information.

Syntax

reset mld-snooping router-port { **all** | **vlan** *vlan-id* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

Examples

Clear information about all dynamic router ports.

```
<Sysname> reset mld-snooping router-port all
```

Related commands

display mld-snooping router-port

reset mld-snooping statistics

Use **reset mld-snooping statistics** to clear statistics for MLD messages learned through MLD snooping.

Syntax

reset mld-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for all MLD messages learned through MLD snooping.

```
<Sysname> reset mld-snooping statistics
```

Related commands

display mld-snooping statistics

router-aging-time (MLD-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

Related commands

mld-snooping router-aging-time

version (MLD-snooping view)

Use **version** to specify an MLD snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The MLD snooping version in a VLAN is 1.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable MLD snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in MLD-snooping view or for a VLAN in VLAN view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable MLD snooping for VLAN 2 through VLAN 10, and specify MLD snooping version 2 for these VLANs.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
[Sysname-mld-snooping] version 2 vlan 2 to 10
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping version