HP 5120 EI Switch Series

Command References

Software version: Release 2215

Document version: 6W100-20120428

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

About the HP 5120 EI command references–Release 2215

The HP 5120 EI command references describe the commands and command syntax options available for the HP 5120 EI Switch Series, software release train 2215.

Command Reference	Content
01 Fundamentals Command Reference	Covers the commands for logging in to and setting up the Switch. This command reference includes: • CLI (command privilege settings and CLI management commands) • Login in to the switch • FTP • TFTP client • File system management • Configuration file management • Software upgrade • Device management
02 IRF Command Reference	Covers IRF configuration commands, including IRF port binding, member ID assignment, priority assignment, and MAD.
03 Layer 2 – LAN Switching Command Reference	Covers the commands for configuring Layer 2 technologies and features in a LAN switched network. This command reference includes: • Ethernet interface • Loopback and null interfaces • Bulk configuring interfaces • MAC address table • MAC Information • Ethernet link aggregation • Port isolation • Spanning tree • BPDU tunneling • VLAN • Isolate-user-VLAN • Voice VLAN • GVRP • QinQ • LLDP • MVRP

Command Reference	Content
04 Layer 3 – IP Services Command Reference	Covers the commands for configuring and managing IP addressing (including static and dynamic IPv4 and IPv6 address assignment), IRDP, UDP helper, DNS, network performance optimization, and ARP. This command reference includes: • ARP • Gratuitous ARP • Proxy ARP • ARP snooping • IP addressing • DHCP server • DHCP relay agent • DHCP client • DHCP snooping • BOOTP client • IPv4 DNS • IRDP • IP performance optimization • UDP Helper • IPv6 basics • DHCPv6 • IPv6 DNS
05 Layer 3 – IP Routing Command Reference	Covers the routing configuration commands. This command reference includes: • Basic IP routing commands • Static routing • IPv6 static routing
06 IP Multicast Command Reference	Covers the commands for Layer 2 IPv4 multicast protocols (IGMP snooping, PIM snooping, and multicast VLAN), and Layer 2 IPv6 multicast protocols (MLD snooping, IPv6 PIM snooping, and IPv6 multicast VLAN). This command reference includes: • IGMP snooping • PIM snooping • Multicast VLAN • MLD Snooping • IPv6 PIM snooping • IPv6 multicast VLAN
07 ACL and QoS Command Reference	Covers the commands for classifying traffic with ACLs, and allocating network resources and managing congestions with QoS technologies to improve network performance and network use efficiency. This command reference includes: • ACL • QoS policy • Priority mapping • GTS and line rate • Congestion management • Data buffer

Command Reference	Content
08 Security Command Reference	Covers security feature commands. Available security features include identity authentication (AAA), access security (802.1X, MAC authentication, portal and port security), secure management (SSH), and attack protection (IP source guard and ARP attack protection). This command reference includes: • AAA • 802.1X • EAD fast deployment • MAC authentication • Portal • Port security • User profile • Password control • HABP • Public key • PKI • IPsec • SSH2.0 • SCP • SSL • TCP attack protection • IP source guard • ARP attack protection • ND attack protection • SAVI • Blacklist
09 High Availability Command Reference	Covers high availability commands for managing failure detection and failover. Failure detection technologies focus on fault detection and isolation. Failover technologies focus on network recovery. This command reference includes: • Ethernet OAM • CFD • DLDP • RRPP • Smart Link • Monitor Link • Track

Command Reference	Content
10 Network Management and Monitoring Command Reference	Covers the commands that help you manage and monitor your network, for example, manage system events, sample packets, assess network performance, synchronize the clock for all devices with the clock in the network, supply power for attached devices by using PoE, and test network connectivity. This command reference includes: • System maintenance and debugging • NTP • Information center • SNMP • RMON • Port mirroring • Traffic mirroring • NQA • sFlow • IPC • PoE • Cluster management • Stack management

Contents

CLI configuration commands

command-alias enable

Syntax

command-alias enable

undo command-alias enable

View

System view

Default level

2: System level

Description

Use **command-alias enable** to enable the command keyword alias function.

Use **undo command-alias enable** to disable the command keyword alias function.

By default, the command keyword alias function is disabled.

Disabling the command keyword alias function does not delete the configured aliases, but the aliases do not take effect anymore.

Related commands: **command-alias mapping**.

Examples

# Enable the command keyword alias function.

```
<Sysname> system-view
[Sysname] command-alias enable
```

# Disable the command keyword alias function.

```
<Sysname> system-view
[Sysname] undo command-alias enable
```

command-alias mapping

Syntax

command-alias mapping *cmdkey alias*

undo command-alias mapping *cmdkey*

View

System view

Default level

2: System level

Parameters

cmdkey: Complete form of the first keyword of a non-undo command, or the second keyword of an **undo** command.

alias: Alias for the keyword, which must be different from the first keyword of any non-undo command.

Description

Use **command-alias mapping** to configure a command keyword alias.

Use **undo command-alias mapping** to delete a command keyword alias.

By default, a command keyword has no alias.

Command keyword aliases take effect only after you enable the command keyword alias function.

Examples

# Define **show** as the alias of the **display** keyword.

```
<Sysname> system-view
[Sysname] command-alias mapping display show
```

After you configure the alias, you can enter **show** to execute a **display** command. For example, you can enter **show clock** to execute the **display clock** command.

# Delete the alias of the **display** keyword.

```
<Sysname> system-view
[Sysname] undo command-alias mapping display
```

command-privilege

Syntax

command-privilege level *level* **view** *view command*

undo command-privilege view *view command*

View

System view

Default level

3: Manage level

Parameters

level *level*: Command level, which ranges from 0 to 3.

view *view*: Specifies a view.

command: Command to be set in the specified view.

Description

Use **command-privilege** to assign a level for a specific command in a view.

Use **undo command-privilege** to restore the default.

By default, each command in a view has a specified level.

Command levels include four privileges: visit (0), monitor (1), system (2), and manage (3). You can assign a privilege level according to the user's need. When logging in to the device, the user can access the assigned level and all levels below it.

Level changes can cause maintenance, operation, and security problems. HP recommends using the default command level or modifying the command level under the guidance of professional staff.

The *command* specified for the **command-privilege** command must be complete, and have valid parameters. For example, the default level of the **tftp** *server-address* { **get** | **put** | **sget** } *source-filename*

[*destination-filename*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] command is 3. To enable users with the privilege level 0 to execute the **tftp** *server-address* **put** *source-filename* command (such as **tftp 192.168.1.26 put syslog.txt**) and disable them from specifying the **get**, **sget**, **source**, or *destination-filename* option, configure the **command-privilege level 0 view shell tftp 1.1.1.1 put a.cfg** command.

The *command* specified for the **undo command-privilege view** command can be incomplete. For example, configuring the **undo command-privilege view system ftp** command restores all commands starting with **ftp** (such as **ftp server acl**, **ftp server enable**, and **ftp timeout**) to their default level. If you have modified the level of commands **ftp server enable** and **ftp timeout**, and you want to restore only the **ftp server enable** command to its default level, use the **undo command-privilege view system ftp server** command.

If you change the command level of a command in a specified view from the default command level to a lower level, you must change the command levels of the **quit** command and the command used to enter this view. For example, the default command level of commands **interface** and **system-view** is 2 (system level). To make the **interface** command available to the level 1 users, execute the following commands: **command-privilege level 1 view shell system-view**, **command-privilege level 1 view system interface gigabitethernet1/0/1**, and **command-privilege level 1 view system quit**. Then, the level 1 users can enter system view, execute the **interface gigabitethernet** command, and return to user view.

Examples

# Set the command level of the **interface** command to 0 in system view.

```
<Sysname> system-view
[Sysname] command-privilege level 0 view system interface
```

display clipboard

Syntax

display clipboard [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display clipboard** to display data in the clipboard.

To copy some content to the clipboard:

1. Move the cursor to the starting position of the content, and then press the **Esc+Shift+,** combination.
2. Move the cursor to the ending position of the content, and then press the **Esc+Shift+.** combination.

Examples

# Display data in the clipboard.

```
<Sysname> display clipboard
---------------- CLIPBOARD-----------------
display current-configuration
```

display command-alias

Syntax

display command-alias [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display command-alias** to display the command keyword alias configuration.

Examples

# Display the command keyword alias configuration.

```
<Sysname> display command-alias
Command alias is enabled
index  alias                         command key
1      show                          display
```

display history-command

Syntax

display history-command [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display history-command** to display commands saved in the command history buffer.

By default, the system can save up to 10 commands in the buffer. You can use the **history-command max-size** command to change the buffer size.

Examples

# Display all commands saved in the command history buffer.

```
<Sysname> display history-command
  display history-command
  system-view
  vlan 2
  quit
```

display hotkey

Syntax

display hotkey [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display hotkey** to display hotkey information.

Examples

# Display hotkey information.

```
<Sysname> display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
```

```
CTRL_L  display ip routing-table
CTRL_O  undo debug all

           =Undefined hotkeys=
Hotkeys Command
CTRL_T  NULL
CTRL_U  NULL

            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

hotkey

Syntax

hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command*

undo hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** }

View

System view

Default level

2: System level

Parameters

CTRL_G: Assigns a command to **Ctrl+G**.

CTRL_L: Assigns a command to **Ctrl+L**.

CTRL_O: Assigns a command to **Ctrl+O**.

CTRL_T: Assigns a command to **Ctrl+T**.

CTRL_U: Assigns a command to **Ctrl+U**.

command: Command to be assigned to the hotkey.

Description

Use **hotkey** to assign a command to a configurable hotkey.

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

By default:

- **Ctrl_G**: **display current-configuration** (display the running configuration)
- **Ctrl_L**: **display ip routing-table** (display the IPv4 routing table information)
- **Ctrl_O**: **undo debugging all** (disable all debugging functions)
- **Ctrl_T**: No command is assigned to this hotkey.
- **Ctrl_U**: No command is assigned to this hotkey.

Examples

# Assign the **display tcp status** command to the hotkey **Ctrl+T**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp status
```

quit

Syntax

quit

View

Any view

Default level

0: Visit level (executed in user view)

2: System level (executed in other views)

Description

Use **quit** to return to the upper-level view.

In user view, this command disconnects you from the device.

Examples

# Return from GigabitEthernet 1/0/1 interface view to system view and then to user view.

```
[Sysname-Gigabitethernet1/0/1] quit
[Sysname] quit
<Sysname>
```

return

Syntax

return

View

Any view except user view

Default level

2: System level

Description

Use **return** to return to user view from any other view. Pressing **Ctrl+Z** has the same effect.

Related commands: **quit**.

Examples

# Return to user view from GigabitEthernet 1/0/1 interface view.

```
[Sysname-Gigabitethernet1/0/1] return
<Sysname>
```

screen-length disable

Syntax

screen-length disable

undo screen-length disable

View

User view

Default level

1: Monitor level

Description

Use **screen-length disable** to disable pausing between screens of output for the current session.

Use **undo screen-length disable** to enable pausing between screens of output for the current session.

By default, a login user uses the settings of the **screen-length** command. The default settings of the **screen-length** command are: pausing between screens of output and displaying up to 24 lines on a screen.

When the screen pause function is disabled, all output is displayed at one time and the screen is refreshes continuously.

This command only takes effect for the current session. When you log out, the setting by this command is restored to the default.

Related commands: **screen-length**.

Examples

# Disable pausing between screens of output for the current session.

```
<Sysname> screen-length disable
```

super

Syntax

super [*level*]

View

User view

Default level

0: Visit level

Parameters

level: User level, which ranges from 0 to 3 and defaults to 3.

Description

Use **super** to switch from the current user privilege level to a specified user privilege level.

If a *level* is not specified, the command switches the user privilege level to 3.

There are four user privilege levels: visit (0), monitor (1), system (2), and manage (3). You can assign different privilege levels to different users. After login, a user can access the commands at or under the assigned level.

A user can switch to a lower privilege level unconditionally. To switch to a higher privilege level, an AUX user interface user (logged in through the console port) does not need to provide any password, but a VTY user must enter the switching password set with the **super password** command. If the entered password is incorrect or no password is configured for switching to the level, the switching operation fails.

Related commands: **super password** and **super authentication-mode**.

Examples

# Switch to user privilege level 2 from user privilege level 3.

```
<Sysname> super 2
User privilege level is 2, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

# Switch back to user privilege level 3 (suppose the switching password is **123**. If no password is set, users cannot switch to user privilege level 3).

```
<Sysname> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

super authentication-mode

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

View

System view

Default level

2: System level

Parameters

local: Uses the local password set with the **super password** command for user privilege level switching authentication. If no password is set with the command, the system allows a console port user to switch the privilege level without authentication, but denies the switching requests of VTY users.

scheme: Uses AAA for user privilege level switching authentication. For more information about AAA, see *Security Configuration Guide*.

local scheme: Uses the local password, if configured, for user privilege level switching authentication. If the password is not configured, the system allows a console port user to switch the privilege level but uses AAA to authenticate VTY users.

scheme local: Uses AAA for user privilege level switching authentication. If the AAA configuration is incomplete or invalid or the server does not respond, the system uses the local password for the authentication.

Description

Use **super authentication-mode** to set the authentication mode for user privilege level switching.

Use **undo super authentication-mode** to restore the default.

By default, the authentication mode for the user privilege level switching is **local**.

Related commands: **super password**.

Examples

# Set the authentication mode for the user privilege level switching to **local**.

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

# Set the authentication mode for the user privilege level switching to **scheme local**.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

super password

Syntax

super password [**level** *user-level*] { **cipher** | **simple** } *password*

undo super password [**level** *user-level*]

View

System view

Default level

2: System level

Parameters

level *user-level*: User privilege level, which ranges from 1 to 3 and defaults to 3.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Description

Use **super password** to set the password used to switch from the current user privilege level to a higher one.

Use **undo super password** to restore the default.

By default, no password is set for switching to a higher privilege level.

Whether you specify the **cipher** or **simple** keyword, the password is saved in cipher text in the configuration file.

Examples

# Use the password **abc** in plain text to authenticate a user switching to privilege level **3**.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

system-view

Syntax

system-view

View

User view

Default level

2: System level

Description

Use **system-view** to enter system view from user view.

Related commands: **quit** and **return**.

Examples

# Enter system view from user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

Login management commands

acl (user interface view)

Syntax

To use a basic or advanced ACL:

acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

To use an Ethernet frame header ACL:

acl *acl-number* **inbound**

undo acl *acl-number* **inbound**

View

VTY user interface view

Default level

2: System level

Parameters

ipv6: When this keyword is present, the command supports IPv6; otherwise, it supports IPv4.

acl-number: Number of the access control list (ACL):

- **Basic ACL**—2000 to 2999
- **Advanced ACL**—3000 to 3999
- **Ethernet frame header ACL**—4000 to 4999

inbound: Restricts Telnet or SSH connections established in the inbound direction through the VTY user interface. If the received packets for establishing a Telnet or SSH connection are permitted by an ACL rule, the connection is allowed to be established. When the device functions as a Telnet server or SSH server, this keyword is used to control access of Telnet clients or SSH clients.

outbound: Restricts Telnet connections established in the outbound direction through the VTY user interface. If the packets sent for establishing a Telnet connection are permitted by an ACL rule, the connection is allowed to be established. When the device functions as a Telnet client, this keyword is used to define Telnet servers accessible to the client.

Description

Use **acl** to reference ACLs to control access to the VTY user interface.

Use **undo acl** to cancel the ACL application. For more information about ACL, see *ACL and QoS Configuration Guide*.

By default, access to the VTY user interface is not restricted.

If no ACL is referenced in VTY user interface view, the VTY user interface has no access control over establishing a Telnet or SSH connection.

If an ACL is referenced in VTY user interface view, the connection is permitted to be established only when packets for establishing a Telnet or SSH connection match a permit statement in the ACL.

The system regards the basic/advanced ACL with the **inbound** keyword, the basic/advanced ACL with the **outbound** keyword, and Ethernet frame header ACL as different types of ACLs, which can coexist in one VTY user interface. The match order is basic/advanced ACL, Ethernet frame header ACL. At most one ACL of each type can be referenced in the same VTY user interface, and the last configured one takes effect.

Examples

# Allow only the user with the IP address of 192.168.1.26 to access the device through Telnet or SSH.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 192.168.1.26 0
[Sysname-acl-basic-2001] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 2001 inbound
```

After your configuration, user A (with IP address 192.168.1.26) can Telnet to the device while user B (with IP address 192.168.1.60) cannot Telnet to the device. Upon a connection failure, a message appears, saying "%connection closed by remote host!"

# Allow the device to only Telnet to the Telnet server with IP address 192.168.1.41.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit tcp destination 192.168.1.41 0
[Sysname-acl-adv-3001] quit
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] acl 3001 outbound
[Sysname-ui-vty0-15] return
<Sysname>
```

After your configuration, if you Telnet to 192.168.1.46, your operation fails.

```
<Sysname> telnet 192.168.1.46
%Can't access the host from this terminal!
```

But you can Telnet to 192.168.1.41.

```
<Sysname> telnet 192.168.1.41
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
```

activation-key

Syntax

activation-key *character*

undo activation-key

View

User interface view

Default level

3: Manage level

Parameters

character: Shortcut key for starting a terminal session, a single character (or its corresponding ASCII code value that ranges from 0 to 127) or a string of 1 to 3 characters. However, only the first character functions as the shortcut key. For example, if you input an ASCII code value of 97, the system uses its corresponding character **a** as the shortcut key. If you input string b@c, the system uses the first character **b** as the shortcut key.

Description

Use **activation-key** to define a shortcut key for starting a terminal session.

Use **undo activation-key** to restore the default.

By default, pressing the **Enter** key starts a terminal session. However, if a new shortcut key is defined with the **activation-key** command, the **Enter** key no longer functions. To display the shortcut key you have defined, use the **display current-configuration | include activation-key** command.

This **activation-key** command is not supported for VTY user interfaces.

Examples

# Configure character **s** as the shortcut key for starting a terminal session on the console port.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] activation-key s
```

# Verify the configuration.

1. Exit the terminal session on the console port.

   ```
   [Sysname-ui-aux0] return
   <Sysname> quit
   ```

2. Log in to the console port again.

   The following message appears.

   ```
   ******************************************************************************
   * Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
   * Without the owner's prior written consent,                                 *
   * no decompiling or reverse-engineering shall be allowed.                    *
   ******************************************************************************


   User interface aux0 is available.




   Please press ENTER.
   ```

3. Press **Enter**.

   At this moment, pressing **Enter** does not start a session.

4. Enter **s**.

   A terminal session is started.

   ```
   <Sysname>
   %Mar  2 18:40:27:981 2011 Sysname SHELL/5/LOGIN: Console login from aux0
   ```

auto-execute command

Syntax

auto-execute command *command*

undo auto-execute command

View

User interface view

Default level

3: Manage level

Parameters

command: Specifies a command to be automatically executed.

Description

Use **auto-execute command** to specify a command to be automatically executed when a user logs in to the current user interface.

Use **undo auto-execute command** to remove the configuration.

By default, command auto-execution is disabled.

The **auto-execute command** command is not supported by the AUX user interface.

The system automatically executes the specified command when a user logs in to the user interface, and tears down the user connection after the command is executed. If the command triggers another task, the system does not tear down the user connection until the task is completed.

Typically, you can use the **auto-execute command** *telnet* command in user interface view to enable a user to automatically Telnet to the specified host when the user logs in to the device. After the user terminates the connection with the host, the user's connection with the device is automatically terminated.

IMPORTANT:

The **auto-execute command** command may disable you from configuring the system through the user interface to which the command is applied. Before configuring the command and saving the configuration (by using the **save** command), make sure that you can access the device through VTY or AUX user interfaces to remove the configuration when a problem occurs.

Examples

# Configure the device to automatically Telnet to 192.168.1.41 after a user logs in to interface VTY 0.

```
<Sysname> system-view
 [Sysname] user-interface vty 0
[Sysname -ui-vty0] auto-execute command telnet 192.168.1.41
% This action will lead to configuration failure through ui-vty0. Are you sure?
[Y/N]:y
[Sysname-ui-vty0]
```

To verify the configuration, Telnet to 192.168.1.40. The device automatically Telnets to 192.168.1.41. The following output is displayed:

```
C:\> telnet 192.168.1.40
******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
```

```
******************************************************************************

<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
```

This operation is the same as directly logging in to the device at 192.168.1.41. If the Telnet connection to 192.168.1.41 is broken down, the Telnet connection to 192.168.1.40 breaks down at the same time.

authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

View

User interface view

Default level

3: Manage level

Parameters

none: Performs no authentication.

password: Performs local password authentication.

scheme: Performs AAA authentication. For more information about AAA, see *Security Configuration Guide*.

Description

Use **authentication-mode** to set the authentication mode for the user interface.

Use **undo authentication-mode** to restore the default.

By default, the authentication mode for VTY user interfaces is **password**, and for AUX user interfaces is **none**.

Related commands: **set authentication password**.

Examples

# Specify that no authentication is needed for VTY 0. (This mode is insecure.)

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

# Use password authentication when users log in to the device through VTY 0, and set the authentication password to **321**.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password cipher 321
```

# Authenticate users by username and password for VTY 0. Set the username to **123** and the password to **321**.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
[Sysname] local-user 123
[Sysname-luser-123] password cipher 321
[Sysname-luser-123] service-type telnet
[Sysname-luser-123] authorization-attribute level 3
```

command accounting

Syntax

command accounting

undo command accounting

View

User interface view

Default level

3: Manage level

Parameters

None

Description

Use **command accounting** to enable command accounting.

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

By default, command accounting is disabled. The accounting server does not record the commands that users have executed.

When command accounting is enabled and command authorization is not, every executed command is recorded on the HWTACACS server.

When both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.

Examples

# Enable command accounting on VTY 0. Then the HWTACACS server records the commands executed by users that have logged in through VTY 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command accounting
```

command authorization

Syntax

command authorization

undo command authorization

View

User interface view

Default level

3: Manage level

Parameters

None

Description

Use **command authorization** to enable command authorization.

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

By default, command authorization is disabled. Logged-in users can execute commands without authorization.

With command authorization enabled, users can perform only commands authorized by the server.

Examples

# Enable command accounting for VTY 0 so that users logging in from VTY 0 can perform only the commands authorized by the HWTACACS server.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command authorization
```

databits

Syntax

databits { **7** | **8** }

undo databits

View

User interface view

Default level

2: System level

Parameters

7: Sets 7 data bits for each character.

8: Sets 8 data bits for each character.

Description

Use **databits** to set data bits for each character.

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

By default, 8 data bits are set for each character.

This command is only applicable to the asynchronous serial port (console port).

The data bits setting must be the same for the user interfaces of the connecting ports on the device and the terminal device for communication.

Examples

# Specify 7 data bits for each character.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

display ip http

Syntax

display ip http [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip http** to display HTTP information.

Examples

# Display information about HTTP..

```
<Sysname> display ip http
HTTP port: 80
Basic ACL: 0
Current connection: 0
Operation status: Running
```

Table 1 Command output

Field	Description
HTTP port	Port number used by the HTTP service.
Basic ACL	Basic ACL number associated with the HTTP service.
Current connection	Number of current connections.

Field	Description
Operation status	Operation status: • **Running**—The HTTP service is enabled. • **Stopped**—The HTTP service is disabled.

display ip https

Syntax

display ip https [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip https** to display information about HTTPS.

Examples

# Display information about HTTPS.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy:
Certificate access-control-policy:
Basic ACL: 0
Operation status: Stopped
```

Table 2 Command output

Field	Description
HTTPS port	Port number used by the HTTPS service.
SSL server policy	The SSL server policy associated with the HTTPS service.
Certificate access-control-policy	The certificate attribute access control policy associated with the HTTPS service.
Basic ACL	The basic ACL number associated with the HTTPS service.
Current connection	Number of current connections.

Field	Description
Operation status	Operation status: • **Running**—The HTTPS service is enabled. • **Stopped**—The HTTPS service is disabled.

display telnet client configuration

Syntax

display telnet client configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display telnet client configuration** to display the configuration of the device when it serves as a Telnet client.

Examples

# Display the configuration of the device when it serves as a Telnet client.

```
<Sysname> display telnet client configuration
 The source IP address is 1.1.1.1.
```

The output shows that when the device serves as a client, the source IPv4 address for sending Telnet packets is 1.1.1.1.

display user-interface

Syntax

display user-interface [*num1* | { **aux** | **vty** } *num2*] [**summary**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

num1: Absolute number of a user interface, in the range of 0 to 35.

aux: Specifies the AUX user interface.

vty: Specifies the VTY user interface.

num2: Relative number of a user interface, in the range of 0 to 3 for an AUX user interface and in the range of 0 to 15 for a VTY user interface.

summary: Displays summary about user interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display user-interface** to display information about the specified or all user interfaces.

If the **summary** keyword is not included, the command displays the type of the user interface, absolute or relative number, transmission rate, user privilege level, authentication mode, and the access port.

If the **summary** keyword is included, the command displays all the numbers and types of user interfaces.

Examples

# Display summary about all user interfaces.

```
<Sysname> display user-interface summary
  User interface type : [AUX]
            0:UXXX
  User interface type : [VTY]
           20:XXXX XXXX XXXX XXXX

    1 character mode users.    (U)
   19 UI never used.        (X)
    1 total UI in use
```

Table 3 Command output

Field	Description
User interface type	Type of user interface, AUX, VTY.
0:X	0 represents the absolute number of the user interface. X means this user interface is not used; U means this user interface is in use.
character mode users. (U)	Number of users, or, the total number of character U.
UI never used. (X)	Number of user interfaces not used, or, the total number of character X.
total UI in use	Total number of user interfaces in use.

display users

Syntax

display users [**all**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information about all user interfaces that the device supports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display users** to display information about the user interfaces that are being used.

Use **display users all** to display information about all user interfaces supported by the device.

Examples

# Display information about the user interfaces that are being used.

```
<Sysname> display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
+ 20  VTY 0   00:00:00 TEL  3
  21  VTY 1   00:09:19 TEL  3

Following are more details.
VTY 0   :
        Location: 192.168.1.54
VTY 1   :
        Location: 192.168.1.58
 +    : Current operation user.
 F    : Current operation user work in async mode.
```

The output shows that two users have logged in to the device. The one with IP address 192.168.1.54 uses VTY 0, and the other with IP address 192.168.1.58 uses VTY 1.

Table 4 Command output

Field	Description
Idx	Absolute number of the user interface.

Field	Description
UI	Relative number of the user interface. For example, with VTY, the first column represents user interface type, and the second column represents the relative number of the user interface.
Delay	Time elapsed since the user's last input, in the format of hh:mm:ss.
Type	User type, such as Telnet or SSH.
Userlevel	User level: 0 for visit, 1 for monitor, 2 for system, and 3 for manage.
+	Current user.
Location	IP address of the user.
F	The current user is operating in asynchronous mode.

display web users

Syntax

display web users [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display web users** to display information about the web users.

Examples

# Display information about the web users.

```
<Sysname> display web users
UserID    Name       Language  Level      State     LinkCount LoginTime LastTime
ab800000  admin      Chinese   Management Enable      0       14:13:46  14:14:18
```

Table 5 Command output

Field	Description
UserID	Web user ID
Name	Web username
Language	Language used in web login

Field	Description
Level	Web user level
State	Web user status
LinkCount	Number of tasks running for the web user
LoginTime	Login time
LastTime	Last time when the web user accessed the device

escape-key

Syntax

escape-key { **default** | *character* }

undo escape-key

View

User interface view

Default level

3: Manage level

Parameters

character: Specifies the shortcut key for terminating a task, a single character (or its corresponding ASCII code value in the range of 0 to 127) or a string of 1 to 3 characters. Only the first character of a string functions as the shortcut key. For example, if you enter an ASCII code value of 113, the system uses its corresponding character q as the shortcut key. If you enter the string q@c, the system uses the first character **q** as the shortcut key.

default: Restores the default escape key sequence **Ctrl+C**.

Description

Use **escape-key** to define a shortcut key for terminating a task.

Use **undo escape-key** to disable the shortcut key for terminating tasks.

By default, you can use **Ctrl+C** to terminate a task.

After you define a new shortcut key by using the **escape-key** command, the new shortcut key is used to terminate a task. To display the shortcut key you have defined, use the **display current-configuration** command.

If you set the *character* argument in a user interface to log in to the device and then Telnet to another device, the *character* argument can be used as a control character to terminate a task rather than used as a common character. For example, if you specify *character* **e** in VTY 0 user interface of Device A, when you log in to Device A by using VTY 0 from a PC (Hyper Terminal), you can input **e** as a common character on the PC, and you can also use **e** to terminate the task running on Device A. If you Telnet to Device B from Device A, you can only use **e** to terminate the task running on Device B, rather than use **e** as a common character, so specify *character* as a key combination.

Examples

# Define key **a** as the shortcut key for terminating a task.

```
<Sysname> system-view
[Sysname] user-interface aux 0
```

```
[Sysname-ui-aux0] escape-key a
```

To verify the configuration:

# Ping the IP address of 192.168.1.49 and use the **-c** keyword to specify the number of ICMP echo packets to be sent as 20.

```
<Sysname> ping -c 20 192.168.1.49
  PING 192.168.1.49: 56  data bytes, press a to break
    Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

# Enter **a**. The task terminates immediately and the system returns to system view.

```
  --- 192.168.1.49 ping statistics ---
    2 packet(s) transmitted
    2 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

<Sysname>
```

flow-control

Syntax

flow-control { **hardware** | **none** | **software** }

undo flow-control

View

User interface view

Default level

2: System level

Parameters

hardware: Performs hardware flow control.

none: Disables flow control.

software: Performs software flow control.

Description

Use **flow-control** to configure the flow control mode.

Use **undo flow-control** to restore the default.

By default, the flow control mode is **none**, which means no flow control is performed.

A flow control mode takes effect on both inbound and outbound directions. In inbound flow control, the local device listens to the remote device for flow control information while in the outbound flow control, the local device sends flow control information to the remote device.

Two ends must be configured with the same flow control mode.

This command is only applicable to the asynchronous serial port (console port).

NOTE:

The switch supports the **none** flow control mode only.

Examples

# Configure no flow control in the inbound and outbound directions for AUX 0.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] flow-control none
```

free user-interface

Syntax

free user-interface { *num1* | { **aux** | **vty** } *num2* }

View

User view

Default level

3: Manage level

Parameters

num1: Absolute number of a user interface, in the range of 0 to 35.

aux: Specifies the AUX user interface.

vty: Specifies the VTY user interface.

num2: Relative number of a user interface, in the range of 0 to 3 for an AUX user interface and in the range of 0 to 15 for a VTY user interface.

Description

Use **free user-interface** to release connections established on the specified user interface.

This command cannot release the connection that you are using.

Examples

# Release the connection established on user interface VTY 1.

1. Display the users that are operating the device.

   ```
   <Sysname> display users
   The user application information of the user interface(s):
   + 20  VTY 0   00:00:00 TEL  3
     21  VTY 1   00:09:51 TEL  3
   Following are more details.
   VTY 0   :
           Location: 192.168.0.10
   VTY 1   :
           Location: 192.168.0.5
    +    : Current operation user.
    F    : Current operation user work in async mode.
   ```

2. If the operations of the user using VTY 1 affect the operations of the administrator, log out the user.

   ```
   <Sysname> free user-interface vty 1
   ```

```
Are you sure to free user-interface vty1? [Y/N]:y
```

free web-users

Syntax

free web-users { **all** | **user-id** *user-id* | **user-name** *user-name* }

View

User view

Default level

2: System level

Parameters

all: Specifies all web users.

user-id: Web user ID, which is a hexadecimal number of eight digits.

user-name: Name of the web user. This argument can contain 1 to 80 characters.

Description

Use **free web-users** to log out web users.

Related commands: **display web users**.

Examples

# Log out all web users.

```
<Sysname> free web-users all
```

history-command max-size

Syntax

history-command max-size *size-value*

undo history-command max-size

View

User interface view

Default level

2: System level

Parameters

size-value: Specifies the maximum number of history commands that the buffer can store. The value is in the range of 0 to 256.

Description

Use **history-command max-size** to set the size of the history command buffer of the current user interface.

Use **undo history-command max-size** to restore the default.

By default, the buffer saves 10 history commands.

The history command buffer saves executed history commands per user interface and buffers for different user interfaces do not affect each other. To display the commands that are stored in the history buffer, use the display **history-command** command. To view the recently executed commands, press the upper arrow or lower arrow key.

After you terminate the current session, the system automatically removes the commands saved in the corresponding history buffer.

Examples

# Set the buffer to store 20 history commands at most.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] history-command max-size 20
```

idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

View

User interface view

Default level

2: System level

Parameters

minutes: Specifies the timeout time in minutes, in the range of 0 to 35791. The default value is 10 minutes.

seconds: Specifies timeout time in seconds, in the range of 0 to 59. The default value is 0 seconds.

Description

Use **idle-timeout** to set the idle-timeout timer.

Use **undo idle-timeout** to restore the default.

The default idle-timeout is 10 minutes.

The system automatically terminates the user's connections if there is no information interaction between the device and the users within the idle timeout time.

Setting idle-timeout to zero disables the timer. In this case, connections are maintained unless you terminate them.

Examples

# Set the idle-timeout timer to 1 minute and 30 seconds.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] idle-timeout 1 30
```

ip http acl

Syntax

ip http acl *acl-number*

undo ip http acl

View

System view

Default level

2: System level

Parameters

acl-number: ACL number, in the range of 2000 to 2999.

Description

Use **ip http acl** to associate the HTTP service with an ACL.

Use **undo ip http acl** to remove the association.

By default, the HTTP service is not associated with any ACL.

After the HTTP service is associated with an ACL, only the clients permitted by the ACL can access the device through HTTP.

Related commands: **display ip http**; **acl** (*ACL and QoS Command Reference*).

Examples

# Associate the HTTP service with ACL 2001 to only allow the clients within the 10.10.0.0/16 network to access the device through HTTP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip http acl 2001
```

ip http dscp

Syntax

ip http dscp *dscp-value*

undo ip http dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **ip http dscp** to set the DSCP value for IPv4 to use for outgoing HTTP packets.

Use **undo ip http dscp** to restore the default.

By default, IPv4 uses the DSCP value 16 for outgoing HTTP packets.

Examples

# Set the DSCP value for IPv4 to use for outgoing HTTP packets to 30.

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

```
[Sysname] ip http dscp 30
```

ip http enable

Syntax

ip http enable

undo ip http enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip http enable** to enable the HTTP service.

Use **undo ip http enable** to disable the HTTP service.

The device can act as the HTTP server that can be accessed only after the HTTP service is enabled.

By default, the HTTP service is enabled.

Related commands: **display ip http**.

Examples

# Enable the HTTP service.

```
<Sysname> system-view
[Sysname] ip http enable
```

# Disable the HTTP service.

```
<Sysname> system-view
[Sysname] undo ip http enable
```

ip http port

Syntax

ip http port *port-number*

undo ip http port

View

System view

Default level

3: Manage level

Parameters

port-number: Port number of the HTTP service, in the range of 1 to 65535.

Description

Use **ip http port** to configure the port number of the HTTP service.

Use **undo ip http port** to restore the default.

By default, the port number of the HTTP service is 80.

Verify that the port number is not used by another service, because this command does not check for conflicts with configured port numbers.

Related commands: **display ip http**.

Examples

# Configure the port number of the HTTP service as 8080.

```
<Sysname> system-view
[Sysname] ip http port 8080
```

ip https acl

Syntax

ip https acl *acl-number*

undo ip https acl

View

System view

Default level

3: Manage level

Parameters

acl-number: ACL number, in the range of 2000 to 2999.

Description

Use **ip https acl** to associate the HTTPS service with an ACL.

Use **undo ip https acl** to remove the association.

By default, the HTTPS service is not associated with any ACL.

After the HTTPS service is associated with an ACL, only the clients permitted by the ACL can access the device.

Related commands: **display ip https**; **acl** (*ACL and QoS Command Reference*).

Examples

# Associate the HTTPS service with ACL 2001 to only allow the clients within the 10.10.0.0/16 network segment to access the HTTPS server through HTTP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip https acl 2001
```

ip https certificate access-control-policy

Syntax

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

View

System view

Default level

3: Manage level

Parameters

policy-name: Name of the certificate attribute access control policy, a string of 1 to 16 characters.

Description

Use **ip https certificate access-control-policy** to associate the HTTPS service with a certificate attribute access control policy.

Use **undo ip https certificate access-control-policy** to remove the association.

By default, the HTTPS service is not associated with any certificate attribute access control policy.

Association of the HTTPS service with a certificate attribute access control policy can control the access rights of clients.

Related commands: **display ip https**; **pki certificate access-control-policy** (*Security Command Reference*).

Examples

# Associate the HTTPS server to certificate attribute access control policy **myacl**.

```
<Sysname> system-view
[Sysname] ip https certificate access-control-policy myacl
```

ip https enable

Syntax

ip https enable

undo ip https enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use ip https enable to enable the HTTPS service.

Use **undo ip https enable** to disable the HTTPS service.

By default, the HTTPS service is disabled.

The device can act as the HTTP server that can be accessed only after the HTTP service is enabled.

Enabling the HTTPS service triggers an SSL handshake negotiation process.

If the local certificate of the device exists, the SSL negotiation succeeds, and the HTTPS service can be started.

If no local certificate exists, the SSL negotiation triggers a certificate application process that often fails because it times out. If that happens, execute the **ip https enable** command multiple times to start the HTTPS service.

Related commands: **display ip https**.

Examples

# Enable the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https enable
```

ip https port

Syntax

ip https port *port-number*

undo ip https port

View

System view

Default level

3: Manage level

Parameters

port-number: Port number of the HTTPS service, in the range of 1 to 65535.

Description

Use **ip https port** to configure the port number of the HTTPS service.

Use **undo ip https port** to restore the default.

By default, the port number of the HTTPS service is 443.

Verify that the port number is not used by another service, because this command does not check for conflicts with configured port numbers.

Related commands: **display ip https**.

Examples

# Configure the port number of the HTTPS service as 6000.

```
<Sysname> system-view
[Sysname] ip https port 6000
```

ip https ssl-server-policy

Syntax

ip https ssl-server-policy *policy-name*

undo ip https ssl-server-policy

View

System view

Default level

3: Manage level

Parameters

policy-name: Name of an SSL server policy, a string of 1 to 16 characters.

Description

Use **ip https ssl-server-policy** to associate the HTTPS service with an SSL server-end policy.

Use **undo ip https ssl-server-policy** to remove the association.

By default, the HTTPS service is not associated with any SSL server-end policy.

The HTTPS service can be enabled only after this command is configured successfully.

With the HTTPS service enabled, you cannot modify the associated SSL server-end policy or remove the association between the HTTPS service and the SSL server-end policy after the HTTPS service is enabled.

Related commands: **display ip https**; **ssl server-policy** (*Security Command Reference*).

Examples

# Associate the HTTPS service with SSL server-end policy **myssl**.

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

ipv6 http dscp

Syntax

ipv6 http dscp *dscp-value*

undo ipv6 http dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **ipv6 http dscp** to set the DSCP value for IPv6 to use for outgoing HTTP packets.

Use **undo ipv6 http dscp** to restore the default.

By default, IPv6 uses the DSCP value 0 for outgoing HTTP packets.

Examples

# Set the DSCP value for IPv6 to use for outgoing HTTP packets to 30.

```
<Sysname> system-view
[Sysname] ipv6 http dscp 30
```

lock

Syntax

lock

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **lock** to lock the user interface. This method prevents unauthorized users from using the user interface.

When entering the **lock** command, you are asked to input a password (up to 16 characters) and then confirm it by inputting the password again. After locking the user interface, you must press **Enter** and input the correct password next time you enter this user interface.

By default, this function is disabled.

Examples

# Lock the current user interface.

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interface:
Password:
Again:







                   locked !




Password:
<Sysname>
```

parity

Syntax

parity { **even** | **none** | **odd** }

undo parity

View

User interface view

Default level

2: System level

Parameters

even: Performs an even parity check.

none: Performs no parity check.

odd: Performs an odd parity check.

Description

Use **parity** to set a parity check method.

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

By default, no parity check is performed.

This command is only applicable to the asynchronous serial port (console port).

The parity check setting must be the same for the user interfaces of the connecting ports on the device and the target terminal device for communication.

Examples

# Configure the Console port to perform odd parity check.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity odd
```

protocol inbound

Syntax

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

View

VTY interface view

Default level

3: Manage level

Parameters

all: Supports both protocols: Telnet and SSH.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Description

Use **protocol inbound** to enable the current user interface to support either Telnet, SSH, or all of them. The configuration takes effect next time you log in.

Use **undo protocol inbound** to restore the default.

By default, both protocols are supported.

Before configuring a user interface to support SSH, set the authentication mode to **scheme** for the user interface; otherwise, the **protocol inbound ssh** command fails. For more information, see **authentication-mode**.

By default, the authentication mode of the Telnet protocol is **password**.

Examples

# Enable the VTYs 0 through 4 to support SSH only.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

screen-length

Syntax

screen-length *screen-length*

undo screen-length

View

User interface view

Default level

2: System level

Parameters

screen-length: Number of lines to be displayed on the screen, in the range of 0 to 512. The value of 0 disables pausing between screens of output.

Description

Use **screen-length** to set the number of lines to be displayed on the screen.

Use **undo screen-length** to restore the default.

By default, the screen displays 24 lines.

When screen output pauses, press the **Space** key to display the next screen. Not all terminals support this command setting. For example, assume that you set *screen-length* to 40, but the terminal can display 24 lines in one screen at most. When you press **Space**, the device sends 40 lines to the terminal, but the next screen displays only lines 18 through 40. To view the first 17 lines, you must press the page up or page down key.

To disable multiple-screen output for the current user interface, use the **screen-length disable** command.

Examples

# Set the next screen of the AUX user interface 0 to display 30 lines.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] screen-length 30
```

send

Syntax

send { **all** | *num1* | { **aux** | **vty** } *num2* }

View

User view

Default level

1: Monitor level

Parameters

all: Sends messages to all user interfaces.

aux: Specifies the AUX user interface.

vty: Specifies the VTY user interface.

num1: Absolute number of a user interface, in the range of 0 to 35.

num2: Relative number of a user interface, in the range of 0 to 3 for an AUX user interface and in the range of 0 to 15 for a VTY user interface.

Description

Use **send** to send messages to the specified user interfaces.

To end message input, press **Ctrl**+**Z**. To cancel message input and return to user view, press **Ctrl**+**C**.

Examples

# Send message **hello abc** to the AUX user interface 0.

```
<Sysname> send aux 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello abc^Z
Send message? [Y/N]:y
<Sysname>

***
***
***Message from aux0 to aux0
***
hello abc



<Sysname>
```

# Assume you are using VTY 0. Before you restart the device, to inform users that are accessing the device through other user interfaces, perform the following steps.

1. Display information about all users

   ```
   <Sysname> display users
     Idx UI      Delay    Type Userlevel
   + 20  VTY 0   00:00:00 TEL  3
     21  VTY 1   00:00:06 TEL  3

   Following are more details.
   VTY 0   :
           Location: 192.168.1.26
   VTY 1   :
           Location: 192.168.1.20
    +    : Current operation user.
    F    : Current operation user work in async mode.
   ```

   // The output shows that a user is using VTY 0.

2. Send a notification to the user of VTY 1.

   ```
   <Sysname> send vty 1
   Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
   Note please, I will reboot the system in 3 minutes!^Z
   Send message? [Y/N]:y
   ```

   // A message is sent to VTY 1, telling that the system will reboot in 3 minutes.

3. If a user is trying to log in through VTY 1, the message appears. (VTY 1 receives the message from VTY 0 when the **interface GigabitEthernet** command is input.)

   ```
   [Sysname] interface gigabiteth

   ***
   ***
   ***Message from vty0 to vty1
   ***
   Note please, I will reboot the system in 3 minutes!
   ```

set authentication password

Syntax

set authentication password { **cipher** | **simple** } *password*

undo set authentication password

View

User interface view

Default level

3: Manage level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Description

Use **set authentication password** to set a local authentication password.

Use **undo set authentication password** to remove the local authentication password.

By default, no local authentication password is set.

The password, whether specified in plain or cipher text, is always saved to the configuration file in cipher text.

Related commands: **authentication-mode**.

Examples

# Set the local authentication password for the AUX 0 user interface to **hello**.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
```

```
[Sysname-ui-aux0] set authentication password cipher hello
```

Next time you enter the system, the password is required.

shell

Syntax

shell

undo shell

View

User interface view

Default level

3: Manage level

Parameters

None

Description

Use **shell** to enable terminal services on the current user interface.

Use **undo shell** to disable terminal services on the current user interface.

The console port does not support the **undo shell** command.

You cannot disable the terminal services on the user interface through which you are logged in.

By default, terminal services are enabled on all user interfaces.

Examples

# Disable terminal services on VTYs 0 through 15, which means you cannot log in to the device through VTYs 0 through 15.

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] undo shell
% Disable ui-vty0-15 , are you sure? [Y/N]:y
[Sysname-ui-vty0-15]
```

The following message appears when a terminal tries to Telnet to the device:

```
The connection was closed by the remote host!
```

speed (user interface view)

Syntax

speed speed-value

undo speed

View

User interface view

Default level

2: System level

Parameters

speed-value: Transmission rate in bps. The transmission rates available with asynchronous serial interfaces include: 300 bps, 600 bps, 1200 bps, 2400 bps, 4800 bps, 9600 bps, 19200 bps, 38400 bps, 57600 bps, and 115200 bps. The transmission rate varies with devices and configuration environment.

Description

Use **speed** to set the transmission rate on the user interface.

Use **undo speed** to restore the default transmission rate.

By default, the transmission rate is 9600 bps.

This command is only applicable to the asynchronous serial port (console port).

The transmission rate setting must be identical for the user interfaces of the connecting ports on the device and the target terminal device for communication.

Examples

# Set the transmission rate on the AUX 0 user interface to 19200 bps.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 19200
```

stopbits

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

View

User interface view

Default level

2: System level

Parameters

1: One stop bit.

1.5: One and a half stop bits.

2: Two stop bits.

Description

Use **stopbits** to set the number of stop bits transmitted per byte.

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

By default, the stop bit is one.

This command is only applicable to the asynchronous serial port (console port).

The stop bits setting must be the identical for the user interfaces of the connecting ports on the device and the target device for communication.

Examples

# Set the stop bits on the user interface AUX 0 to 1.5.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 1.5
```

telnet

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]

View

User view

Default level

0: Visit level

Parameters

remote-host: IPv4 address or host name of a remote host, a case-insensitive string of 1 to 20 characters.

service-port: TCP port number of the Telnet service on the remote host. It is in the range of 0 to 65535 and defaults to 23.

source: Specifies the source interface or source IPv4 address of Telnet packets.

interface *interface-type interface-number*: Specifies the source interface. The source IPv4 address of the Telnet packets sent is the IPv4 address of the specified interface. *interface-type interface-number* represents the interface type and number.

ip *ip-address*: Specifies the source IPv4 address of Telnet packets.

Description

Use **telnet** to Telnet to a remote host.

To terminate the current Telnet connection, press **Ctrl+K** or use the **quit** command.

The source IPv4 address or source interface specified by this command is applicable to the current Telnet connection only.

Examples

# Telnet to the remote host 1.1.1.2, specifying the source IP address of Telnet packets as 1.1.1.1.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

telnet client dscp

Syntax

telnet client dscp *dscp-value*

undo telnet client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **telnet client dscp** to set the DSCP value for IPv4 to use for outgoing Telnet packets on a Telnet client.

Use **undo telnet client dscp** to restore the default.

By default, IPv4 uses the DSCP value 16 for outgoing Telnet packets on a Telnet client.

Examples

# Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet client.

```
<Sysname> system-view
[Sysname] telnet client dscp 30
```

telnet client ipv6 dscp

Syntax

telnet client ipv6 dscp *dscp-value*

undo telnet client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **telnet client ipv6 dscp** to set the DSCP value for IPv6 to use for outgoing Telnet packets on a Telnet client.

Use **undo telnet client ipv6 dscp** to restore the default.

By default, IPv6 uses the DSCP value 0 for outgoing Telnet packets on a Telnet client.

Examples

# Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet client.

```
<Sysname> system-view
[Sysname] telnet client ipv6 dscp 30
```

telnet client source

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

View

System view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies the source interface. The source IPv4 address of the Telnet packets sent is the IPv4 address of the specified interface. *interface-type interface-number* represents the interface type and number.

ip *ip-address*: Specifies the source IPv4 address of Telnet packets.

Description

Use **telnet client source** to specify the source IPv4 address or source interface for sending Telnet packets when the device serves as a Telnet client.

Use **undo telnet client source** to remove the source IPv4 address or source interface for sending Telnet packets.

By default, no source IPv4 address or source interface for sending Telnet packets is specified. The source IPv4 address is selected by routing.

The source IPv4 address or source interface specified by this command is applicable all Telnet connections.

If you use both this command and the **telnet** command to specify the source IPv4 address or source interface, the source IPv4 address or interface specified by the **telnet** command takes effect.

Related commands: **display telnet client configuration**.

Examples

# Specify the source IPv4 address for sending Telnet packets when the device serves as a Telnet client as 1.1.1.1.

```
<Sysname> system-view
[Sysname] telnet client source ip 1.1.1.1
```

telnet ipv6

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*]

View

User view

Default level

0: Visit level

Parameters

remote-host: IP address or host name of a remote host, a case-insensitive string of 1 to 46 characters.

-i *interface-type interface-number*: Specifies the outbound interface for sending Telnet packets, where *interface-type interface-number* represents the interface type and number. If the destination address is a link-local address, provide the **–i** *interface-type interface-number* argument.

port-number: TCP port number for the remote host to provide the Telnet service. It is in the range of 0 to 65535 and defaults to 23.

Description

Use **telnet ipv6** to Telnet to a remote host in an IPv6 network. To terminate the current Telnet connection, press **Ctrl+K** or use the **quit** command.

Examples

# Telnet to the remote host with the IPv6 address 5000::1.

```
<Sysname> telnet ipv6 5000::1
```

telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **telnet server dscp** to set the DSCP value for IPv4 to use for outgoing Telnet packets on a Telnet server.

Use **undo telnet server dscp** to restore the default.

By default, IPv4 uses the DSCP value 48 for outgoing Telnet packets on a Telnet server.

Examples

# Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

telnet server enable

Syntax

telnet server enable

undo telnet server enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **telnet server enable** to enable the Telnet server.

Use **undo telnet server enable** to disable the Telnet server.

The Telnet server is enabled by default.

Examples

# Enable the Telnet server.

```
<Sysname> system-view
[Sysname] telnet server enable
```

telnet server ipv6 dscp

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **telnet server ipv6 dscp** to set the DSCP value for IPv6 to use for outgoing Telnet packets on a Telnet server.

Use **undo telnet server ipv6 dscp** to restore the default.

By default, IPv6 uses the DSCP value 0 for outgoing Telnet packets on a Telnet server.

Examples

# Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

terminal type

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

View

User interface view

Default level

2: System level

Parameters

ansi: Specifies the terminal display type as ANSI.

vt100: Specifies the terminal display type as VT100.

Description

Use **terminal type** to configure the type of terminal display of the current user interface.

Use **undo terminal type** to restore the default.

By default, the terminal display type is ANSI.

The device supports two types of terminal display: ANSI and VT100. HP recommends you to set the display type of both the device and the client to VT100. If the device and the client use different display types (for example, hyper terminal or Telnet terminal) or both are set to ANSI, when the total number of characters of the currently edited command line exceeds 80, an anomaly such as cursor corruption or abnormal display of the terminal display may occur on the client.

Examples

# Set the terminal display type to VT100.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

user privilege level

Syntax

user privilege level *level*

undo user privilege level

View

User interface view

Default level

3: Manage level

Parameters

level: Specifies a user privilege level, in the range of 0 to 3.

Description

Use **user privilege level** to configure the user privilege level. Users logging into the user interface are assigned a user privilege level.

Use **undo user privilege level** to restore the default.

By default, the default command level is 3 for the console user interface and 0 for other user interfaces.

User privilege levels include visit, monitor, system, and manage, represented by the number 0, 1, 2 and 3 respectively. The administrator can change the user privilege level when necessary.

Examples

# Set the command level for users logging in through VTY 0 to 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 0
```

After you Telnet to the device through VTY 0, the terminal only displays commands of level 0 in the help information:

```
<Sysname> ?
```

```
cfd      Connectivity fault detection (IEEE 802.1ag)
cluster  Run cluster command
display  Display current system information
ping     Ping function
quit     Exit from current command view
ssh2     Establish a secure shell client connection
super    Set the current user priority level
telnet   Establish one TELNET connection
tracert  Trace route function
```

user-interface

Syntax

user-interface { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }

View

System view

Default level

2: System level

Parameters

first-num1: Absolute number of the first user interface, in the range of 0 to 35.

last-num1: Absolute number of the last user interface, in the range of 1 to 35, but cannot be smaller than the *first-num1*.

aux: Specifies the AUX user interface.

vty: Specifies the VTY user interface.

first-num2: Relative number of the first user interface, in the range of 0 to 3 for an AUX user interface and in the range of 0 to 15 for a VTY user interface.

last-num2: Relative number of the last user interface, in the range of 1 to 3 for an AUX user interface and in the range of 1 to 15 for a VTY user interface, but cannot be smaller than *first-num 2*.

Description

Use **user-interface** to enter a single or multiple user interface views.

In a single user interface view, the configuration takes effect in the user view only.

In multiple user interface views, the configuration takes effect in these user views.

Examples

# Enter the user interface view of AUX 0.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0]
```

# Enter the user interface views of VTYs 0 to 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4]
```

FTP configuration commands

FTP server configuration commands

display ftp-server

Syntax

display ftp-server [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ftp-server** to display the FTP server configuration.

After configuring FTP server parameters, you may verify them with this command.

Related commands: **ftp server enable**, **ftp timeout**, and **ftp update**.

Examples

# Display the FTP server configuration.

```
<Sysname> display ftp-server
   FTP server is running
   Max user number:              1
   User count:                   1
   Timeout value(in minute):     30
   Put Method:                   fast
```

Table 6 Command output

Field	Description
Max user number	Maximum number of concurrent login users.
User count	Number of the current login users.

Field	Description
Timeout value (in minute)	Allowed idle time of an FTP connection. If there is no packet exchange between the FTP server and client during the time frame, the FTP connection will be disconnected.
Put Method	File update method of the FTP server, **fast** or **normal**.

display ftp-user

Syntax

display ftp-user [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ftp-user** to display the detailed information of current FTP users.

Examples

# Display the detailed information of FTP users.

```
<Sysname> display ftp-user
  UserName             HostIP          Port       Idle             HomeDir
  ftp                  192.168.1.54    1190       0                flash:
```

# If the name of the login user exceeds 10 characters, the excessive characters will be displayed in the next line and left justified. For example, if the user name is **administrator**, the following information will appear:

```
<Sysname> display ftp-user
  UserName             HostIP              Port       Idle             HomeDir
administra
tor                    192.168.0.152       1031       0                flash:
```

Table 7 Command output

Field	Description
UserName	Name of the currently logged-in user
HostIP	IP address of the currently logged-in user
Port	Port which the currently logged-in user is using

Field	Description
Idle	Duration time of the FTP connection, in minutes
HomeDir	Authorized path of the logged-in user

free ftp user

Syntax

free ftp user *username*

View

User view

Default level

3: Manage level

Parameters

username: Username. You can use the **display ftp-user** command to view FTP login user information.

Description

Use **free ftp user** to manually release the FTP connection established by the specified user.

This command releases the FTP connection established by the specified user no matter whether the user is transmitting a file.

Examples

# Manually release the FTP connection established with username **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP user ftpuser? [Y/N]:y
<Sysname>
```

ftp server acl

Syntax

ftp server acl *acl-number*

undo ftp server acl

View

System view

Default level

3: Manage level

Parameters

acl-number: Basic access control list (ACL) number, in the range of 2000 to 2999.

Description

Use **ftp server acl** to use an ACL to control FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

By default, no ACL is used to control FTP clients' access to the FTP server.

An ACL enables the FTP server to permit the FTP requests from specific FTP clients. This configuration only filters the FTP connections to be established, and has no effect on existing FTP connections and operations. If you execute the command multiple times, the last specified ACL takes effect.

Examples

# Associate the FTP service with ACL 2001 to allow only the client 1.1.1.1 to access the FTP server through FTP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-basic-2001] rule 1 deny source any
[Sysname-acl-basic-2001] quit
[Sysname] ftp server acl 2001
```

ftp server dscp

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **ftp server dscp** to set the DSCP value for IP to use for outgoing FTP packets on an FTP server.

Use **undo ftp server dscp** to restore the default.

By default, IP uses the DSCP value 0 for outgoing FTP packets on a FTP server.

Examples

# Set the DSCP value for IP to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server dscp 30
```

ftp server enable

Syntax

ftp server enable

undo ftp server

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **ftp server enable** to enable the FTP server and allow the login of FTP users.

Use **undo ftp server** to disable the FTP server.

By default, the FTP server is disabled.

Examples

# Enable the FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

ftp timeout

Syntax

ftp timeout *minute*

undo ftp timeout

View

System view

Default level

3: Manage level

Parameters

minute: Idle-timeout timer in minutes, in the range of 1 to 35791.

Description

Use **ftp timeout** to set the idle-timeout timer.

Use **undo ftp timeout** to restore the default.

By default, the FTP idle time is 30 minutes.

If the idle time of an FTP connection exceeds the FTP timeout value, the FTP server breaks the connection to save resources.

Examples

# Set the idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

ftp update

Syntax

ftp update { **fast** | **normal** }

undo ftp update

View

System view

Default level

3: Manage level

Parameters

fast: Fast update. In this mode, the FTP server writes the complete file to the memory before writing it to the storage medium.

normal: Normal update. In this mode, the FTP server writes the data of a file from the memory to the storage medium multiple times, with up to 4096 bytes per time.

Description

Use **ftp update** to set the file update mode that the FTP server uses while receiving data.

Use **undo ftp update** to restore the default.

By default, the file update mode is **normal**.

Examples

# Set the FTP update mode to **normal**.

```
<Sysname> system-view
[Sysname] ftp update normal
```

FTP client configuration commands

Before executing the FTP client configuration commands in this section, check that you have configured the proper authority, including view the files under the current directory, read/download the specified file, create directory/upload files, and rename/remove files) for users on the FTP server.

The prompt information for the examples varies with FTP server types.

ascii

Syntax

ascii

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **ascii** to set the file transfer mode to ASCII.

By default, the file transfer mode is ASCII.

The carriage return characters vary with operating systems. For example, HP and Windows use characters **/r/n**, and Linux uses characters **/n**. To transfer files between two systems that use different carriage return characters, determine FTP transfer mode according to the file type.

FTP transfers files in the following modes:

- **Binary mode**—for program file or picture transmission.
- **ASCII mode**—for text file transmission.

Related commands: **binary**.

Examples

# Set the file transfer mode to ASCII.

```
[ftp] ascii
200 Type set to A.
```

binary

Syntax

binary

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **binary** to set the file transfer mode to binary (flow) mode.

By default, the transfer mode is ASCII mode.

Related commands: **ascii**.

Examples

# Set the file transfer mode to **binary**.

```
[ftp] binary
200 Type set to I.
```

bye

Syntax

bye

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **bye** to disconnect from the remote FTP server and return to user view.

If no connection is established between the device and the remote FTP server, use this command to return to user view directly.

Related commands: **close**, **disconnect**, and **quit**.

Examples

# Terminate the connection with the remote FTP server and return to user view.

```
[ftp] bye
221 Server closing.
```

cd

Syntax

cd { *directory* | **..** | **/** }

View

FTP client view

Default level

3: Manage level

Parameters

directory: Name of the target directory, in the format of [*drive*:][/]*path,* where *drive* represents the storage medium name, typically flash. If no drive information is provided, the argument represents a folder or subfolder in the current directory. For more information about the *drive* and *path* arguments, see *Fundamentals Configuration Guide.*

..: Returns to an upper directory. The execution of the **cd ..** command equals the execution of the **cdup** command. If the current working directory is the root directory, or no upper directory exists, the current working directory does not change when the **cd ..** command is executed. This argument does not support command line online help.

/: Returns to the root directory of the storage medium. The keyword does not support command line online help.

Description

Use **cd** to change the current working directory on the remote FTP server to access another authorized directory.

Related commands: **pwd**.

Examples

# Change the working directory to the sub-directory **logfile** of the current directory.

```
[ftp] cd logfile
250 CWD command successful.
```

# Change the working directory to the sub-directory **folder** of the authorized directory.

```
[ftp] cd /folder
250 CWD command successful.
```

cdup

Syntax

cdup

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **cdup** to exit the directory and enter the upper directory of the FTP server.

This command does not change the working directory if the directory is **work-directory**.

Related commands: **cd** and **pwd**.

Examples

# Change the working directory path to the upper directory.

```
[ftp] pwd
257 "/ftp/subdir" is current directory.
[ftp] cdup
200 CDUP command successful.
[ftp] pwd
257 "/ftp" is current directory.
```

close

Syntax

close

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **close** to terminate the connection to the FTP server, but remain in FTP client view.

This command is equal to the **disconnect** command.

Examples

# Terminate the connection to the FTP server and remain in FTP client view.

```
[ftp] close
221 Server closing.
[ftp]
```

debugging

Syntax

debugging

undo debugging

View

FTP client view

Default level

1: Monitor level

Parameters

None

Description

Use **debugging** to enable FTP client debugging.

Use **undo debugging** to disable FTP client debugging.

By default, FTP client debugging is disabled.

Examples

# The device serves as the FTP client. Enable FTP client debugging and use the active mode to download file **sample.file** from the current directory of the FTP server.

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> ftp 192.168.1.46
Trying 192.168.1.46 ...
Press CTRL+K to abort
Connected to 192.168.1.46.
220 FTP service ready.
User(192.168.1.46:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]undo passive
FTP: passive is off

[ftp] debugging
FTP: debugging switch is on

[ftp] get sample.file

---> PORT 192,168,1,44,4,21
200 Port command okay.
 The parsed reply is 200
---> RETR sample.file
150 Opening ASCII mode data connection for /sample.file.
 The parsed reply is 150
```

```
FTPC: File transfer started with the signal light turned on.
FTPC: File transfer completed with the signal light turned off.
.226 Transfer complete.
FTP: 3304 byte(s) received in 4.889 second(s), 675.00 byte(s)/sec.

[ftp]
```

Table 8 Command output

Field	Description
---> PORT	Give an FTP order, with data port numbers being…
The parsed reply is	The received reply code, defined in RFC 959.
---> RETR	Download the file.
FTPC: File transfer started with the signal light turned on.	File transfer starts, and the signal light is turned on.
FTPC: File transfer completed with the signal light turned off.	File transfer is completed, and the signal light is turned off.

delete

Syntax

delete *remotefile*

View

FTP client view

Default level

3: Manage level

Parameters

remotefile: File name.

Description

Use **delete** to permanently delete a specified file on the remote FTP server.

To perform this operation, you must have delete permissions on the FTP server.

Examples

# Delete file **temp.c**.

```
[ftp] delete temp.c
250 DELE command successful.
```

dir

Syntax

dir [*remotefile* [*localfile*]]

View

FTP client view

Default level

3: Manage level

Parameters

remotefile: Name of the file or directory on the remote FTP server.

localfile: Name of the local file to save the displayed information.

Description

Use **dir** to view the detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use **dir** *remotefile* to display the detailed information of the specified file or directory on the remote FTP server.

Use **dir** *remotefile localfile* to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile* argument.

The **ls** command can only display the names of files and directories. The **dir** command can display other related information of the files and directories, such as the size, and the date they were created.

Examples

# View the detailed information of the files and subdirectories under the current directory on the remote FTP server.

```
[ftp] dir
227 Entering Passive Mode (192,168,1,46,5,68).
125 ASCII mode data connection already open, transfer starting for /*.
drwxrwxrwx   1 noone    nogroup         0 Aug 08  2006 logfile
-rwxrwxrwx   1 noone    nogroup  20471748 May 11 10:21 test.bin
-rwxrwxrwx   1 noone    nogroup      4001 Dec 08  2007 config.cfg
-rwxrwxrwx   1 noone    nogroup      3608 Jun 13  2007 startup.cfg
drwxrwxrwx   1 noone    nogroup         0 Dec 03  2007 test
-rwxrwxrwx   1 noone    nogroup       299 Oct 15  2007 key.pub
226 Transfer complete.
FTP: 394 byte(s) received in 0.189 second(s), 2.00K byte(s)/sec.

[ftp]
```

# View the information of the file **ar-router.cfg**, and save the result to **aa.txt**.

```
[ftp] dir ar-router.cfg aa.txt
227 Entering Passive Mode (192,168,1,50,17,158).
125 ASCII mode data connection already open, transfer starting for /ar-router.cfg.
....226 Transfer complete.
FTP: 67 byte(s) received in 4.600 second(s), 14.00 byte(s)/sec.
```

# View the content of **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
-rwxrwxrwx   1 noone    nogroup      3077 Jun 20 15:34 ar-router.cfg
```

disconnect

Syntax

disconnect

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **disconnect** to disconnect from the remote FTP server but remain in FTP client view.

This command is equal to the **close** command.

Examples

# Disconnect from the remote FTP server but remain in FTP client view.

```
[ftp] disconnect
221 Server closing.
[ftp]
```

display ftp client configuration

Syntax

display ftp client configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ftp client configuration** to display the source IP address configuration of the FTP client.

This command displays the source IP address configuration of the FTP client. If the specified source IP address is active, this command displays the source IP address. If the specified source interface is active, this command displays the source interface.

Related commands: **ftp client source**.

Examples

# Display the source IP address configuration of the FTP client.

```
<Sysname> display ftp client configuration
 The source IP address is 192.168.0.123
```

ftp

Syntax

ftp [*server-address* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]]

View

User view

Default level

3: Manage level

Parameters

server-address: IP address or host name (a string of 1 to 20 characters) of a remote FTP server.

service-port: TCP port number of the remote FTP server, in the range of 0 to 65535. The default value is 21.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]: Specifies the source address used to establish an FTP connection.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted FTP packets. If no primary IP address is configured on the source interface, the connection fails.
- **ip** *source-ip-address*: Specifies the source IP address of the transmitted FTP packets. This source address must be the one that has been configured on the device.

Description

Use **ftp** to log in to the remote FTP server and enter FTP client view.

This command applies to IPv4 networks only.

If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to the FTP server.

If you specify the parameters, you will be prompted to enter the username and password for accessing the FTP server.

Examples

# Log in the server 192.168.0.211. The source IP address of sent FTP packets is 192.168.0.212.

```
<Sysname1> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 FTP Server ready.
User(192.168.0.211:(none)):abc
331 Password required for abc
```

```
Password:
230 User logged in.

[ftp]
```

ftp client dscp

Syntax

ftp client dscp *dscp-value*

undo ftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **ftp client dscp** to set the DSCP value for IPv4 to use for outgoing FTP packets on an FTP client.

Use **undo ftp client dscp** to restore the default.

By default, IPv4 uses the DSCP value 0 for outgoing FTP packets on an FTP client.

Examples

# Set the DSCP value for IPv4 to use for outgoing FTP packets to 30 on an FTP client.

```
<Sysname> system-view
[Sysname] ftp client dscp 30
```

ftp client ipv6 dscp

Syntax

ftp client ipv6 dscp *dscp-value*

undo ftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **ftp client ipv6 dscp** to set the DSCP value for IPv6 to use for outgoing FTP packets on an FTP client.

Use **undo ftp client ipv6 dscp** to restore the default.

By default, IPv6 uses the DSCP value 0 for outgoing FTP packets on an FTP client.

Examples

# Set the DSCP value for IPv6 to use for outgoing FTP packets to 30 on an FTP client.

```
<Sysname> system-view
[Sysname] ftp client ipv6 dscp 30
```

ftp client source

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

View

System view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies the source interface for establishing FTP connections. The primary IP address of the source interface is used as the source IP address of packets sent to an FTP server. If the source interface has no primary IP address specified, no FTP connection can be established.

ip *source-ip-address*: Specifies the source IP address of packets sent to an FTP server, which is one of the IP addresses of the device.

Description

Use **ftp client source** to specify the source IP address of packets sent to an FTP server.

Use **undo ftp client source** to restore the default.

By default, the source IP address is the IP address of the output interface of the route to the server is used as the source IP address.

If you use the **ftp client source** command to first configure a source interface and then a source IP address, the source IP address overwrites the source interface, and vice versa.

If you first use the **ftp client source** command to specify a source IP address and then use the **ftp** command to specify another source IP address, the latter is used.

The source IP address specified with the **ftp client source** command applies to all FTP connections while the one specified with the **ftp** command applies to the current FTP connection only.

Related commands: **display ftp client configuration**.

Examples

# Specify the source IP address of packets sent to an FTP server as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

# Specify the IP address of interface VLAN-interface 1 as the source IP address of packets sent to an FTP server.

```
<Sysname> system-view
[Sysname] ftp client source interface vlan-interface 1
```

ftp ipv6

Syntax

ftp ipv6 [*server-address* [*service-port*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

View

User view

Default level

3: Manage level

Parameters

server-address: IP address or host name of the remote FTP server.

service-port: TCP port number of the FTP server, in the range of 0 to 65535. The default value is 21.

source ipv6 *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This parameter can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For the configuration of link local addresses, see *Layer 3—IP Services Configuration Guide*.

Description

Use **ftp ipv6** to log in to the FTP server and enter FTP client view.

This command applies to IPv6 networks only.

If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to an FTP server.

If you specify the parameters, enter the username and password for accessing the FTP server.

Examples

# Log in to the FTP server with IPv6 address 3000::200.

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

Default level

3: Manage level

Parameters

remotefile: Name of the file to be downloaded.

localfile: File name used after a file is downloaded and saved locally. If this argument is not specified, the local file uses the name of the source file on the FTP server by default.

Description

Use **get** to download a file from a remote FTP server and save it.

Examples

# Download file **testcfg.cfg** to the root directory of the storage medium of the master, and save it as **newest.cfg**.

```
[ftp] get testcfg.cfg newest.cfg

227 Entering Passive Mode (192,168,1,46,4,47).
125 ASCII mode data connection already open, transfer starting for /testcfg.cfg.
..226 Transfer complete.
FTP: 3608 byte(s) received in 2.050 second(s), 1.00K byte(s)/sec.
```

# Download file **testcfg.cfg** to the root directory of the storage medium of the subordinate device (with the member ID 2), and save it as **newest.cfg**.

```
[ftp] get testcfg.cfg slot2#flash:/newest.cfg

227 Entering Passive Mode (192,168,1,46,4,48).
125 ASCII mode data connection already open, transfer starting for /testcfg.cfg.
226 Transfer complete.
FTP: 3608 byte(s) received in 2.322 second(s), 1.00K byte(s)/sec.
```

lcd

Syntax

lcd

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **lcd** to display the local working directory of the FTP client.

Examples

# Display the local working directory.

```
[ftp] lcd
FTP: Local directory now flash:/clienttemp.
```

The output shows that the working directory of the FTP client before execution of the **ftp** command is **flash:/clienttemp**.

ls

Syntax

ls [*remotefile* [*localfile*]]

## View

FTP client view

Default level

3: Manage level

Parameters

remotefile: Filename or directory on the remote FTP server.

localfile: Name of a local file used to save the displayed information.

Description

Use **ls** to view the information of all the files and subdirectories in the current directory of the remote FTP server. The file names and subdirectory names are displayed.

Use **ls** *remotefile* to view the information of a specified file or subdirectory.

Use **ls** *remotefile localfile* to view the information of a specified file or subdirectory, and save the result to a local file specified by the *localfile* argument.

The **ls** command can only display the names of files and directories on the FTP server. The **dir** command can display other related information of the files and directories, such as the size and the date they were created.

Examples

# View the information of all files and subdirectories in the current directory of the FTP server.

```
[ftp] ls
227 Entering Passive Mode (192,168,1,50,17,165).
125 ASCII mode data connection already open, transfer starting for /*.
ar-router.cfg
logfile
mainar.bin
arbasic.bin
ftp
test
bb.cfg
testcfg.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.
```

# View the information of directory **logfile**, and save the result to file **aa.txt**.

```
[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,46,4,3).
125 ASCII mode data connection already open, transfer starting for /logfile/*.
....226 Transfer complete.
FTP: 20 byte(s) received in 3.962 second(s), 5.00 byte(s)/sec.
```

# View the content of file **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
.
..
logfile.log
```

mkdir

Syntax

mkdir *directory*

## View

FTP client view

Default level

3: Manage level

Parameters

directory: Name of the directory to be created.

Description

Use **mkdir** to create a subdirectory in the current directory on the remote FTP server.

You must have permissions on the FTP server.

Examples

# Create subdirectory **mytest** on the current directory of the remote FTP server.

```
[ftp] mkdir mytest
257 "/mytest" new directory created.
```

open

Syntax

open *server-address* [*service-port*]

## View

FTP client view

Default level

3: Manage level

Parameters

server-address: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range of 0 to 65535. The default value is 21.

Description

Use **open** to log in to the IPv4 FTP server under FTP client view.

At login, enter the username and password. If your input is correct, the login succeeds.

If you have logged in to the IPv4 FTP server, you cannot use the **open** command to log in to another server. To do so, you must disconnect from the current server first.

Related commands: **close**.

Examples

# In FTP client view, log in to the FTP server with the IP address of 192.168.1.50.

```
<Sysname> ftp
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

open ipv6

Syntax

open ipv6 *server-address* [*service-port*] [**-i** *interface-type interface-number*]

View

FTP client view

Default level

3: Manage level

Parameters

server-address: IP address or host name of the remote FTP server.

service-port: Port number of the remote FTP server, in the range of 0 to 65535. The default value is 21.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This parameter can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For the configuration of link local addresses, see *Layer 3—IP Services Configuration Guide*.

Description

Use **open ipv6** to log in to the IPv6 FTP server in FTP client view.

At login, enter the username and password for accessing the FTP server. If your input is correct, the login succeeds.

Related commands: **close**.

Examples

# Log in to the FTP server (with IPv6 address 3000::200) in FTP client view.

```
<Sysname> ftp
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
```

passive

Syntax

passive

undo passive

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **passive** to set the data transmission mode to **passive**.

Use **undo passive** to set the data transmission mode to **active**.

The default transmission mode is **passive**.

Data transmission modes fall into the passive mode and the active mode. In active mode, the FTP server initiates a data connection request. In passive mode, the FTP client initiates a data connection request. This command is mainly used in conjunction with a firewall to restrict FTP session establishment between private and public network users.

Examples

# Set the data transmission mode to **passive**.

```
[ftp] passive
FTP: passive is on
```

put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

Default level

3: Manage level

Parameters

localfile: Name of the local file to be uploaded.

remotefile: File name used after a file is uploaded and saved on the FTP server.

Description

Use **put** to upload a file on the client to the remote FTP server.

By default, if no name is assigned to the file to be saved on the FTP server, the name of the source file is used.

When a file is uploaded, it is saved in the user's authorized directory, which can be set with the **authorization-attribute** command on the remote server.

Examples

# Upload source file **vrpcfg.cfg** on the master to the remote FTP server and save it as **ftpclient.cfg**.

```
[ftp] put vrpcfg.cfg ftpclient.cfg
227 Entering Passive Mode (192,168,1,46,4,50).
125 ASCII mode data connection already open, transfer starting for /ftpclient.cfg.
226 Transfer complete.
FTP: 1366 byte(s) sent in 0.064 second(s), 21.00Kbyte(s)/sec.
```

# Upload source file **a.cfg** on the subordinate device (with the member ID 2) to the remote FTP server and save it as **ftpclienta.cfg**.

```
[ftp] put slot2#flash:/a.cfg ftpclienta.cfg
227 Entering Passive Mode (192,168,1,46,4,52).
125 ASCII mode data connection already open, transfer starting for /ftpclienta.cfg.
226 Transfer complete.
FTP: 1226 byte(s) sent in 0.065 second(s), 18.00Kbyte(s)/sec.
```

pwd

Syntax

pwd

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **pwd** to display the working directory on the remote FTP server.

Examples

# Display the working directory on the remote FTP server.

```
[ftp] cd servertemp
[ftp] pwd
257 "/servertemp" is current directory.
```

The output shows that the **servertemp** folder under the root directory of the remote FTP server is being accessed by the user.

quit

Syntax

quit

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **quit** to disconnect the FTP client from the remote FTP server and exit to user view.

Examples

# Disconnect from the remote FTP server and exit to user view.

```
[ftp] quit
221 Server closing.

<Sysname>
```

remotehelp

Syntax

remotehelp [*protocol-command*]

View

FTP client view

Default level

3: Manage level

Parameters

protocol-command: FTP command.

Description

Use **remotehelp** to display the help information of FTP-related commands supported by the remote FTP server.

If no argument is specified, FTP-related commands supported by the remote FTP server are displayed.

Examples

# Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp
214-Here is a list of available ftp commands
    Those with '*' are not yet implemented.
   USER   PASS   ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*
   PORT   PASV   TYPE   STRU*  MODE*  RETR   STOR   STOU*
   APPE*  ALLO*  REST*  RNFR*  RNTO*  ABOR*  DELE   RMD
   MKD    PWD    LIST   NLST   SITE*  SYST   STAT*  HELP
   NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD
214 Direct comments to HP company.
```

# Display the help information for the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>.

[ftp]
```

Table 9 Command output

Field	Description
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file

Field	Description
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory
LIST	List files
NLST	List file description
SITE*	Locate a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the **user** command: user (keyword) + space + *username*

rmdir

Syntax

rmdir *directory*

View

FTP client view

Default level

3: Manage level

Parameters

directory: Directory name on the remote FTP server.

Description

Use **rmdir** to remove a specified directory from the FTP server.

Only authorized users are allowed to use this command.

Delete all files and subdirectories under a directory before you delete the directory. For how to delete files, see the **delete** command.

When you execute the **rmdir** command, the files in the remote recycle bin in the directory will be automatically deleted.

Examples

# Delete the **temp1** directory from the authorized directory on the FTP server.

```
[ftp] rmdir /temp1
200 RMD command successful.
```

user

Syntax

user *username* [*password*]

View

FTP client view

Default level

3: Manage level

Parameters

username: Login username.

password: Login password. You can input this argument a space after the *username* argument; or you can input this argument when the "Password:" prompt appears after you input the username and then press **Enter**.

Description

Use **user** to relog in again to the FTP server with another username.

Before using this command, you must configure the corresponding username and password on the FTP server or the login will fail and the FTP connection will close.

Examples

# User **ftp1** has logged in to the FTP server. Use username **ftp2** to log in to the current FTP server. (Suppose username **ftp2** and password **123123123123** have been configured on the FTP server).

- Method 1:

  ```
  [ftp] user ftp2
  331 Password required for ftp2.
  Password:
  230 User logged in.

  [ftp]
  ```

- Method 2

  ```
  [ftp] user ftp2 123123123123
  331 Password required for ftp.
  230 User logged in.

  [ftp]
  ```

verbose

Syntax

verbose

undo verbose

View

FTP client view

Default level

3: Manage level

Parameters

None

Description

Use **verbose** to enable display of detailed prompt information received from the server.

Use **undo verbose** to disable display of detailed prompt information.

By default, the display of detailed prompt information is enabled.

Examples

# Enable display of detailed prompt information.

```
[ftp] verbose
FTP: verbose is on
```

# Disable display of detailed prompt information and perform a Get operation.

```
[ftp] undo verbose
FTP: verbose is off

[ftp] get startup.cfg bb.cfg

FTP: 3608 byte(s) received in 0.052 second(s), 69.00K byte(s)/sec.

[ftp]
# Enable display of detailed prompt information. and perform a Get operation.
[ftp] verbose
FTP: verbose is on

[ftp] get startup.cfg aa.cfg

227 Entering Passive Mode (192,168,1,46,5,85).
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
226 Transfer complete.
FTP: 3608 byte(s) received in 0.193 second(s), 18.00K byte(s)/sec.
```

TFTP client configuration commands

display tftp client configuration

Syntax

display tftp client configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tftp client configuration** to display source IP address configuration of the TFTP client.

This command displays the source IP address configuration of the TFTP client. If the specified source IP address is active, this command displays the source IP address. If the specified source interface is active, this command displays the source interface.

Related commands: **tftp client source**.

Examples

# Display the source IP address configuration of the TFTP client.

```
<Sysname> display tftp client configuration
 The source IP address is 192.168.0.123
```

tftp-server acl

Syntax

tftp-server [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

View

System view

Default level

3: Manage level

Parameters

ipv6: References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

acl-number: Number of a basic ACL, in the range of 2000 to 2999.

Description

Use **tftp-server acl** to control the device's access to a specific TFTP server using an ACL.

Use **undo tftp-server acl** to restore the default.

By default, no ACL is used to control the device's access to TFTP servers.

You can use an ACL to deny or permit the device's access to a specific TFTP server.

For more information about ACL, see *ACL and QoS Configuration Guide.*

Examples

# Allow the device to access the TFTP server with the IP address of 1.1.1.1 only (in the IPv4 networking environment).

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

# Allow the device to access the TFTP server with the IP address of 2001::1 only (in the IPv6 networking environment).

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2001::1/128
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

tftp

Syntax

tftp *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]

View

User view

Default level

3: Manage level

Parameters

server-address: IP address or host name of a TFTP server.

get: Downloads a file in normal mode.

put: Uploads a file.

sget: Downloads a file in secure mode.

source-filename: Source file name.

destination-filename: Destination file name.

source: Configures parameters for source address binding.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by TFTP. If no primary IP address is configured on the source interface, the transmission fails.
- **ip** *source-ip-address*: Specifies the source IP address for the current TFTP client to transmit packets. This source address must be an IP address that has been configured on the device.

Description

Use **tftp** to download a specified file from the TFTP server to the local device or upload a specified local file to the TFTP server in an IPv4 network.

Examples

# To upgrade the device, download the **newest.bin** file from the TFTP server with the IP address of 192.168.1.26 and save it to both the root directory on the flash of the master and the root directory on the flash of the subordinate device (with the member ID 2).

```
<Sysname> tftp 192.168.1.26 get newest.bin startup.bin
  .
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait..................
  TFTP:  2737556 bytes received in 13 second(s)
  File downloaded successfully.
```

// Download the file from the TFTP server to the root directory on the flash of the master.

```
<Sysname> tftp 192.168.1.26 get newest.bin slot2#flash:/startup.bin

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP:  2737556 bytes received in 14 second(s)
  File downloaded successfully.
```

// Download the file from the TFTP server to the root directory on the flash of the subordinate device.

tftp client dscp

Syntax

tftp client dscp *dscp-value*

undo tftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **tftp client dscp** to set the DSCP value for IPv4 to use for outgoing TFTP packets on a TFTP client.

Use **undo tftp client dscp** to restore the default.

By default, IPv4 uses the DSCP value 0 for outgoing TFTP packets on a TFTP client.

Examples

# Set the DSCP value for IPv4 to use for outgoing TFTP packets to 30 on a TFTP client.

```
<Sysname> system-view
[Sysname] tftp client dscp 30
```

tftp client ipv6 dscp

Syntax

tftp client ipv6 dscp *dscp-value*

undo tftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Description

Use **tftp client ipv6 dscp** to set the DSCP value for IPv6 to use for outgoing TFTP packets on a TFTP client.

Use **undo tftp client ipv6 dscp** to restore the default.

By default, IPv6 uses the DSCP value 0 for outgoing TFTP packets on a TFTP client.

Examples

# Set the DSCP value for IPv6 to use for outgoing TFTP packets to 30 on a TFTP client.

```
<Sysname> system-view
[Sysname] tftp client ipv6 dscp 30
```

tftp client source

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

View

System view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies the source interface for establishing TFTP connections. The primary IP address of the source interface is used as the source IP address of packets sent to a TFTP server. If the source interface has no primary IP address specified, no TFTP connection can be established.

ip *source-ip-address*: Specifies the source IP address of packets sent to a TFTP server, which is one of the IP addresses configured on the device.

Description

Use **tftp client source** to specify the source IP address of packets sent to a TFTP server.

Use **undo tftp client source** to restore the default.

By default, the source IP address is the IP address of the output interface of the route to the server is used as the source IP address..

If you use the **tftp client source** command to first configure a source interface and then a source IP address, the source IP address overwrites the source interface, and vice versa.

If you first use the **tftp client source** command to specify a source IP address and then use the **tftp** command to specify another source IP address, the latter is used.

The source IP address specified with the **tftp client source** command applies to all TFTP connections while the one specified with the **tftp** command applies to the current TFTP connection only.

Related commands: **display tftp client configuration**.

Examples

# Specify the source IP address of packets sent to a TFTP server as 2.2.2.2.

```
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2
```

# Specify the IP address of interface VLAN-interface 1 as the source IP address of packets sent to a TFTP server.

```
<Sysname> system-view
[Sysname] tftp client source interface vlan-interface 1
```

tftp ipv6

Syntax

tftp ipv6 *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]

View

User view

Default level

3: Manage level

Parameters

tftp-ipv6-server: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This parameter can be used only when the TFTP server address is a link local address and the specified output interface has a link local address. For the configuration of a link local address, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

get: Downloads a file.

put: Uploads a file.

source-file: Source filename.

destination-file: Destination filename. If it is not specified, this filename is the same as the source filename.

Description

Use **tftp ipv6** to download a specified file from a TFTP server or upload a specified local file to a TFTP server in an IPv6 network.

Examples

# Download **filetoget.txt** from the TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i Vlan-interface 1 get filetoget.txt
  ...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait....
  TFTP:      411100 bytes received in 2 second(s)
  File downloaded successfully.
```

File system management commands

In the following examples, the current working directory is the root directory of the storage medium on the device.

For the qualified filename formats, see *Fundamentals Configuration Guide*.

cd

Syntax

cd { *directory* | **..** | **/** }

View

User view

Default level

3: Manage level

Parameters

directory: Name of the target directory, in the format of [*drive*:/]*path*. For the detailed introduction to the drive and path arguments, see *Fundamentals Configuration Guide.* If no drive information is provided, the argument represents a folder or subfolder in the current directory.

..: Returns to an upper directory. If the current working directory is the root directory, or if no upper directory exists, the current working directory does not change when the **cd ..** command is executed. This argument does not support command online help.

/: Returns to the root directory of the storage medium. This keyword does not support command line online help.

Description

Use **cd** to change the current working directory.

Examples

# Enter the root directory of the flash on a subordinate device with the member ID 2 after logging in to the master.

```
<Sysname> cd slot2#flash:/
```

# Change the current directory from the file system of the subordinate device to the **test** folder in the root directory of the master.

```
<Sysname> cd flash:/
```

copy

Syntax

copy *fileurl-source fileurl-dest*

View

User view

Default level

3: Manage level

Parameters

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file or folder.

Description

Use **copy** to copy a file.

If you specify a target folder, the system will copy the file to the specified folder and use the name of the source file as the file name.

Examples

# Copy the configuration file of the master to the root directory of a subordinate device (with the member ID 2).

```
<Sysname> copy vrcfg.cfg slot2#flash:/
Copy flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg?[Y/N]:y

%Copy file flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg...Done.
```

delete

Syntax

delete [/**unreserved**] *file-url*

View

User view

Default level

3: Manage level

Parameters

/**unreserved**: Permanently deletes the specified file, and the deleted file can never be restored.

file-url: Name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the extension of **.txt** in the current directory, you may use the **delete** *.txt command.

Description

Use **delete** *file-url* to temporarily delete a file. The deleted file is saved in the recycle bin. To restore it, use the **undelete** command.

Use **dir /all** to display the files deleted from the directory and moved to the recycle bin. These files are enclosed in pairs of brackets [ ].

Use **reset recycle-bin** to remove the files from the recycle bin.

Use **delete /unreserved** *file-url* to permanently delete a file, and the deleted file cannot be restored. Use it with caution.

IMPORTANT:

If you delete two files with the same filename in different directories, only the last one is retained in the recycle bin.

Examples

# Remove file **tt.cfg** from the root directory of the storage medium on the master.

```
<Sysname> delete tt.cfg
.
Delete flash:/tt.cfg?[Y/N]:y
.
%Delete file flash:/tt.cfg...Done.
```

# Remove file **tt.cfg** from the root directory of the storage medium on a subordinate device (with the member ID 2).

- Approach 1

  ```
  <Sysname> delete slot2#flash:/tt.cfg
  Delete slot2#flash:/tt.cfg?[Y/N]:y
  %Delete file slot2#flash:/tt.cfg...Done.
  ```

- Approach 2

  ```
  <Sysname> cd slot2#flash:/
  <Sysname> delete tt.cfg
  Delete slot2#flash:/tt.cfg?[Y/N]:y
  %Delete file slot2#flash:/tt.cfg...Done.
  ```

dir

Syntax

dir [/**all**] [*file-url* | /**all-filesystems**]

View

User view

Default level

3: Manage level

Parameters

/**all**: Displays all files and folders in the current directory, including hidden files, hidden folders, files moved from the current directory to the recycle bin. Files in the recycle bin are enclosed in square brackets [ ].

file-url: Displays the specified file. Asterisks (*) are acceptable as wildcards. For example, to display files with the **.txt** extension in the current directory, you may use the **dir** *.txt command.

/**all-filesystems**: Displays files and folders in the root directory of all storage media on the device.

Description

Use **dir** to display files or folders.

If no parameter is specified, the command displays all visible files and folders in the current directory.

Examples

# Display information about all files and folders in the storage medium of the master. (The output depends on your switch model.)

```
<Sysname> dir /all
Directory of flash:/
```

```
   0     -rw-      7380  Mar 25 2011 10:47:36   patch-package.bin
   1     -rw-       228  Mar 25 2011 10:50:39   patchstate
   2     -rwh      2884  Apr 01 2011 17:56:14   private-data.txt
   3     -rw-      3921  Apr 01 2011 17:56:30   startup.cfg
   4     -rw-  12955373  Apr 01 2011 15:24:20   backup.bin
   5     -rw-       151  Apr 01 2011 17:56:24   system.xml

15240 KB total (2517 KB free)
```

# Display files and folders in the root directory of all storage media on the IRF fabric. (The output depends on your switch model.)

```
<Sysname> dir /all-filesystems
Directory of flash:/

   0     -rw-  12948314  Dec 11 2011 15:15:00   main.bin
   1     drw-         -  Apr 26 2011 12:00:54   seclog
   2     -rw-       168  Apr 26 2011 12:09:25   patchstate
   3     -rw-    551510  Apr 26 2011 12:49:44   cmdtree.txt
   4     -rw-       287  Apr 26 2011 12:07:42   system.xml
   5     -rw-      2550  Apr 26 2011 12:07:46   startup.cfg
   6     -rw-      3801  Apr 26 2011 12:03:43   stp.cfg
   7     -rw-    262104  Apr 26 2011 12:05:28   default.diag
15240 KB total (4458 KB free)

Directory of slot1#flash:/

   0     -rw-  12948314  Dec 11 2011 15:15:00   main.bin
   1     -rw-    453420  Apr 26 2011 12:04:52   b59.diag
   2     drw-         -  Apr 26 2011 12:00:18   seclog
   3     -rw-   1540516  Apr 26 2011 15:25:27   b83.diag
   4     -rw-       287  Apr 26 2011 12:05:04   system.xml
   5     -rw-     21009  Apr 26 2011 12:05:19   startup.cfg
   6     -rw-       168  Apr 01 2011 23:55:39   patchstate

15240 KB total (4217 KB free)
```

# Display information about all files and folders in the storage medium of a subordinate device (with the member ID 2).

```
<Sysname> cd slot2#flash:/
<Sysname> dir /all
Directory of slot2#flash:/

   0     -rwh      3144  Apr 26 2011 13:45:28   private-data.txt
   1     -rw-      2341  Apr 26 2011 16:36:18   startup.cfg
   2     -rw-       124  Apr 26 2011 12:00:22   patchstate
   3     -rwh       716  Apr 26 2011 14:31:36   hostkey
   4     -rwh         4  Apr 26 2011 14:31:41   snmpboots
   5     -rw-  10187730  Apr 26 2011 12:01:10   startup.bin
   6     -rwh       572  Apr 26 2011 14:31:47   serverkey
   7     -rwh       548  Apr 26 2011 14:31:52   dsakey
```

```
  8      -rw-      3035  Apr 26 2011 13:45:36   new-config.cfg
  9      drw-         -  Apr 26 2011 12:11:53   oldver

15240 KB total (1839 KB free)
```

Table 10 Command output

Field	Description
Directory of	Current working directory.
d	Indicates a directory. If this field does not exist, it indicates a file.
r	Indicates that the file or directory is readable.
w	Indicates that the file or directory is writable.
h	Indicates that the file or directory is hidden.
[ ]	Indicates that the file is in the recycle bin.

execute

Syntax

execute *filename*

View

System view

Default level

2: System level

Parameters

filename: Name of a batch file with a .bat extension. To change the extension of a configuration file to .bat, use the **rename** command.

Description

Use **execute** to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

Do not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.

Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the command cannot be executed, and the system skips this command and goes to the next one.

Each configuration command in a batch file must be a standard configuration command, meaning that the valid configuration information can be displayed with the **display current-configuration** command.

Examples

# Execute the batch file **test.bat** in the root directory.

```
<Sysname> system-view
[Sysname] execute test.bat
```

file prompt

Syntax

file prompt { **alert** | **quiet** }

View

System view

Default level

3: Manage level

Parameters

alert: Enables the system to warn you about operations that may bring undesirable results, including file corruption or data loss.

quiet: Disables the system from warning you about any operation.

Description

Use **file prompt** to set the file system operation mode.

By default, the operation mode is **alert**.

When the operation mode is set to **quiet**, the system does not warn for any file system operation. To avoid misoperation, use the alert mode.

Examples

# Set the file system operation mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Syntax

fixdisk *device*

View

User view

Default level

3: Manage level

Parameters

device: Storage medium name.

Description

Use **fixdisk** to restore the space of a storage medium when it becomes unavailable because of an abnormal operation.

Examples

# Restore the space of the flash.

```
<Sysname> fixdisk flash:
Fixdisk flash: may take some time to complete...
%Fixdisk flash: completed.
```

format

Syntax

format *device*

View

User view

Default level

3: Manage level

Parameters

device: Name of a storage medium (for example Flash).

Description

Use **format** to format a storage medium.

IMPORTANT:

Formatting a storage medium results in loss of all the files on the storage medium and these files cannot be restored. In particular, if a startup configuration file exists on a storage medium, formatting the storage medium results in loss of the startup configuration file.

Examples

# Format the flash.

```
<Sysname> format flash:
All data on flash: will be lost, proceed with format? [Y/N]:y
./
%Format flash: completed.
```

mkdir

Syntax

mkdir *directory*

View

User view

Default level

3: Manage level

Parameters

directory: Name of a folder.

Description

Use **mkdir** to create a folder under a specified directory on the storage medium.

The name of the folder to be created must be unique in the specified directory. Otherwise, you will fail to create the folder in the directory.

To use this command to create a folder, the specified directory must exist. For example, to create folder **flash:/test/mytest**, the **test** folder must exist. Otherwise, you will fail to create the **mytest** folder.

Examples

# Create folder **test** on a subordinate device (with the member ID 2).

```
<Sysname> mkdir slot2#flash:/test
....
%Created dir slot2#flash:/test.
```

more

Syntax

more *file-url*

View

User view

Default level

3: Manage level

Parameters

file-url: File name.

Description

Use **more** to display the contents of the specified file. It indicates that there are more lines than the screen can display.

Pressing **Enter** displays the next line.

Pressing **Space** displays the next screen.

Pressing **Ctrl+C** or any other key exits the display.

This command is valid only for text files.

Examples

# Display the contents of file **testcfg.cfg** on a subordinate device (with the member ID 2).

```
<Sysname> more slot2#flash:/testcfg.cfg

#
 version 5.20, Release 0000
#
 sysname Test
#
  ---- More ----
```

move

Syntax

move *fileurl-source fileurl-dest*

View

User view

Default level

3: Manage level

Parameters

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file or folder.

Description

Use **move** to move a file.

If you specify a target folder, the system will move the source file to the specified folder, with the file name unchanged.

Examples

# Move file **flash:/test/sample.txt** to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt?[Y/N]:y
...
% Moved file flash:/test/sample.txt to flash:/1.txt
```

# Move file **b.cfg** to the subfolder **test2**.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg?[Y/N]:y
.
%Moved file flash:/b.cfg to flash:/test2/b.cfg.
```

pwd

Syntax

pwd

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **pwd** to display the current path.

Examples

# Display the current path.

```
<Sysname> pwd
flash:
```

rename

Syntax

rename *fileurl-source fileurl-dest*

View

User view

Default level

3: Manage level

Parameters

fileurl-source: Name of the source file or folder.

fileurl-dest: Name of the target file or folder.

Description

Use **rename** to rename a file or folder. The target file name must be unique in the current path.

Examples

# Rename file **sample.txt** as **sample.bat**.

```
<Sysname> rename sample.txt sample.bat
Rename flash:/sample.txt to flash:/sample.bat? [Y/N]:y

% Renamed file flash:/sample.txt to flash:/sample.bat
```

reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

Default level

3: Manage level

Parameters

/force: Deletes all files in the recycle bin, including files that cannot be deleted by the command without the **/force** keyword.

Description

Use **reset recycle-bin** to permanently delete the files in the recycle bin in the current directory.

If a file is corrupted, you may not be able to delete the file using the **reset recycle-bin** command. Use the **reset recycle-bin /force** command to delete the corrupted file in the recycle bin forcibly.

The **delete** *file-url* command only moves a file to the recycle bin. To permanently delete the file in the recycle bin, use the **reset recycle-bin** command in the original directory of the file.

The **reset recycle-bin** command deletes files in the current directory and in the recycle bin. If the original path of the file to be deleted is not the current directory, use the **cd** command to enter the original directory of the file, and then execute the **reset recycle-bin** command.

Examples

# Delete file **b.cfg** in the current directory and in the recycle bin.

1. Display all the files in the recycle bin and in the current directory.

```
<Sysname> dir /all
Directory of flash:/
```

```
   0     -rwh      3080  Apr 26 2011 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2011 13:45:36   config.cfg
   2     -rw-   13308645 May 14 2011 10:13:18   main.bin
   3     -rw-      2386  Apr 26 2011 13:30:30   back.cfg
   4     drw-         -  May 08 2011 09:49:25   test
   5     -rwh       716  Apr 24 2011 16:17:30   hostkey
   6     -rwh       572  Apr 24 2011 16:17:44   serverkey
   7     -rw-      2386  May 08 2011 11:14:20   [a.cfg]
   8     -rw-      3608  Dec 03 2011 17:29:30   [b.cfg]

15240 KB total (6730 KB free)
```

//The output shows that the current directory is **flash:**, and there are two files **a.cfg** and **b.cfg** in the recycle bin.

2. Delete file **b.cfg** in the current directory and in the recycle bin.

```
<Sysname> reset recycle-bin
Clear flash:/~/a.cfg ?[Y/N]:n
Clear flash:/~/b.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
......
%Cleared file flash:/~/b.cfg...
```

3. In directory **flash:**, check whether the file **b.cfg** in the recycle bin is deleted.

```
<Sysname> dir /all
Directory of flash:/

   0     -rwh      3080  Apr 26 2011 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2011 13:45:36   config.cfg
   2     -rw-   13308645 May 14 2011 10:13:18   main.bin
   3     -rw-      2386  Apr 26 2011 13:30:30   back.cfg
   4     drw-         -  May 08 2011 09:49:25   test
   5     -rwh       716  Apr 24 2011 16:17:30   hostkey
   6     -rwh       572  Apr 24 2011 16:17:44   serverkey
   7     -rw-      2386  May 08 2011 11:14:20   [a.cfg]

15240 KB total (6734 KB free)
```

// The output shows that file **flash:/b.cfg** is deleted permanently.

# Delete file **aa.cfg** in the subdirectory **test** and in the recycle bin.

4. Enter the subdirectory

```
<Sysname> cd test/
```

5. Check all the files in the subfolder **test**.

```
<Sysname> dir /all
Directory of flash:/test

   0     -rw-      2161  Apr 26 2011 21:22:35   [aa.cfg]

15240 KB total (6734 KB free)
```

// The output shows that only one file exists in the folder, and the file has been moved to the recycle bin.

6. Permanently delete file **test/aa.cfg**.

```
<Sysname> reset recycle-bin
Clear flash:/test/~/aa.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
..
%Cleared file flash:/test/~/aa.cfg...
```

rmdir

Syntax

rmdir *directory*

View

User view

Default level

3: Manage level

Parameters

directory: Name of the folder.

Description

Use **rmdir** to remove a folder.

The folder must be an empty one. If it is not empty, use the **delete** command to delete all files and subfolders under it.

After you execute the **rmdir** command successfully, the files in the recycle bin in the folder will be automatically deleted.

Examples

# Remove the **mydir** folder.

```
<Sysname> rmdir mydir
Rmdir flash:/mydir?[Y/N]:y

%Removed directory flash:/mydir.
```

undelete

Syntax

undelete *file-url*

View

User view

Default level

3: Manage level

Parameters

file-url: Name of the file to be restored.

Description

Use **undelete** to restore a file from the recycle bin.

If another file with the same name exists in the same path, the system prompts you whether to overwrite the original file.

Examples

# Restore file **a.cfg** in directory **flash:** from the recycle bin.

```
<Sysname> undelete a.cfg
Undelete flash:/a.cfg?[Y/N]:y
.....
%Undeleted file flash:/a.cfg.
```

# Restore file **b.cfg** in directory **flash:/test** from the recycle bin.

```
<Sysname> undelete flash:/test/b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.......
%Undeleted file flash:/test/b.cfg.
```

Or, you can use the following steps to restore file **flash:/test/b.cfg**.

```
<Sysname> cd test
<Sysname> undelete b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.....
%Undeleted file flash:/test/b.cfg.
```

Configuration file management commands

archive configuration

Syntax

archive configuration

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **archive configuration** to save the running configuration manually.

When you execute this command, the system saves the running configuration with the specified filename—filename prefix + serial number—to the specified path.

Before executing the **archive configuration** command, you must configure the filename prefix and path for saving configuration files by using the **archive configuration location** command.

With the **archive configuration** command executed, the running configuration is only saved to the master, and the subordinate switches do not perform the saving operation.

Examples

# Save the running configuration manually.

```
<Sysname> archive configuration
Warning: Save the running configuration to an archive file. Continue? [Y/N]: Y
Please wait...
Info: The archive configuration file myarchive_1.cfg is saved.
```

archive configuration interval

Syntax

archive configuration interval *minutes*

undo archive configuration interval

View

System view

Default level

3: Manage level

Parameters

minutes: Specifies the interval for automatically saving the running configuration, in minutes. The value is in the range of 10 to 525,600 (365 days).

Description

Use **archive configuration interval** to enable the automatic saving of the running configuration and set the interval.

Use **undo archive configuration interval** to restore the default.

By default, the system does not automatically save the running configuration.

With this command executed, the system saves the running configuration with the specified filename to the specified path at a specified interval (the value of the *minutes* argument).

Configure an automatic saving interval according to the storage media performance and the frequency of configuration modification:

- If the configuration of the device does not change frequently, HP recommends that you save the running configuration manually as needed
- HP recommends that you save the running configuration manually, or configure automatic saving with an interval longer than 1,440 minutes (24 hours).

Before executing the **archive configuration interval** command, you must configure the filename prefix and path for saving configuration files by using the **archive configuration location** command.

With the **archive configuration interval** command executed, the running configuration is only saved to the master, and the subordinate switches cannot save the configuration. However, the command is also executed on the subordinate switches to ensure the rollback of the configuration after the master is changed.

Examples

# Configure the system to save the running configuration every 60 minutes.

```
<Sysname> system-view
[Sysname] archive configuration interval 60
Info: Archive files will be saved every 60 minutes.
```

archive configuration location

Syntax

archive configuration location *directory* **filename-prefix** *filename-prefix*

undo archive configuration location

View

System view

Default level

3: Manage level

Parameters

directory: The path of the folder for saving configuration files, a case insensitive string of 1 to 63 characters, in the format of storage media name:/[folder name]/subfolder name. The folder must be created before the configuration.

filename-prefix: The filename prefix for saving configuration files, a case insensitive string of 1 to 30 characters (can include letters, numbers, _, and - only).

Description

Use **archive configuration location** to configure the path and filename prefix for saving configuration files.

Use **undo archive configuration location** to restore the default.

By default, the path and filename prefix for saving configuration files are not configured, and the system does not save the configuration file periodically.

Before the running configuration is saved either manually or automatically, the file path and filename prefix must be configured.

If the **undo archive configuration location** command is executed, the running configuration cannot be saved manually or automatically. The configuration done by executing the **archive configuration interval** and **archive configuration max** commands will restore to the default, and clear the saved configuration files.

When the device is operating in active/standby mode, the saving and rollback operations are executed only on the master. After the active/standby switchover, the configuration rollback can take effect on the new master. The **archive configuration location** command configures the path and filename prefix for saving configuration files on both the master and subordinate switches. Before executing this command, verify that the path is available on both the master and the subordinate switches. The path cannot include any member ID.

Examples

# Configure the path and the filename prefix for saving configuration files as **flash:/archive/** and **my_archive** respectively.

1. Create folder **flash:/archive** on the master.

   ```
   <Sysname> mkdir archive
   .
   %Created dir flash:/archive.
   ```

2. Create folder **flash:/archive** on a subordinate switch (with the member ID 2).

   ```
   <Sysname> mkdir slot2#flash:/archive

   %Created dir slot2#flash:/archive.
   ```

3. Configure the path and the filename prefix for saving configuration files.

   ```
   <Sysname> system-view
   [Sysname] archive configuration location flash:/archive filename-prefix my_archive
   ```

4. Configure the path and the filename prefix for saving configuration files.

   ```
   <Sysname> system-view
   [Sysname] archive configuration location flash:/archive filename-prefix my_archive
   ```

archive configuration max

Syntax

archive configuration max *file-number*

undo archive configuration max

View

System view

Default level

3: Manage level

Parameters

file-number: The maximum number of configuration files that can be saved, which ranges from 1 to 10. The value of the *file-number* argument is determined by the memory space. You are recommended to set a comparatively small value for this argument if the available memory space is small.

Description

Use **archive configuration max** to set the maximum number of configuration files that can be saved.

Use **undo archive configuration max** to restore the default.

By default, a maximum of 5 configuration files can be saved.

Because excessive configuration files occupy large memory space, you can use this command to control the number of the files. After the maximum number of configuration files is saved, the system deletes the oldest files when the next file is saved (either automatically or manually). When you change the maximum number of configuration files that can be saved, the exceeded files are not deleted. If the number of the existing configuration files is larger than or equal to the newly configured upper limit, the system deletes the oldest *n* files when the next file is saved, where n = the current number - the newly configured number + 1, for example: if the number of configuration files that have been saved is 7, and the newly configured upper limit is 4, when there is a new configuration file to be saved, the system deletes 4 oldest files, where 4 = 7-4+1.

Before executing this command, configure the path and filename prefix for saving configuration files by using the **archive configuration location** command; otherwise, the execution of this command fails.

If the **undo archive configuration location** command is executed, the maximum number of configuration files that can be saved also restores to the default.

Examples

# Set the maximum number of configuration files that can be saved to 10.

```
<Sysname> system-view
[Sysname] archive configuration max 10
```

backup startup-configuration

Syntax

backup startup-configuration to *dest-addr* [*dest-filename*]

View

User view

Default level

2: System level

Parameters

dest-addr: IP address or name of a TFTP server. The address cannot be an IPv6 address.

dest-filename: Target filename used to save the startup configuration file on the server.

Description

Use **backup startup-configuration** to back up the startup configuration file to a specified TFTP server. If you do not specify this filename, the original filename is used.

This command only backs up the main startup configuration file.

The switch uses TFTP to back up configuration files.

Examples

# Back up the startup configuration file of the switch to the TFTP server with IP address 2.2.2.2, using filename **192-168-1-26.cfg**.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: flash:/startup.cfg
 Bootrom-access enable state: enabled
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backup next startup-configuration file to 2.2.2.2, please wait…finished!
<Sysname>
```

After the above operation, the switch backs up file **test.cfg** to TFTP server 2.2.2.2, where the file is saved as **192-168-1-26.cfg**.

configuration replace file

Syntax

configuration replace file *filename*

View

System view

Default level

3: Manage level

Parameters

filename: Specifies the name of the replacement configuration file for configuration rollback.

Description

Use **configuration replace file** to set configuration rollback.

When this command is executed, the running configuration rolls back to the configuration state based on the specified configuration file (*filename*).

The configuration file specified with the **configuration replace file** *filename* command can only be a configuration file in simple text. Otherwise, errors may occur in configuration rollback.

Examples

# Roll back from the running configuration to a previous configuration state based on a saved configuration file **my_archive_1.cfg**.

```
<Sysname> system-view
[Sysname] configuration replace file my_archive_1.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
```

```
Info: Now replacing the current configuration. Please wait...
Info: Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

display archive configuration

Syntax

display archive configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display archive configuration** to display information about configuration rollback.

Examples

# Display information about configuration rollback.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Saved archive files:
  No. TimeStamp              FileName
  1   Aug 05 2011 20:24:54   my_archive_1.cfg
  2   Aug 05 2011 20:34:54   my_archive_2.cfg
# 3   Aug 05 2011 20:44:54   my_archive_3.cfg
'#' indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Table 11 Command output

Field	Description
Location	Absolute path of the saved configuration files.
Filename prefix	Filename prefix of the saved configuration files.
Archive interval in minutes	Configuration file saving interval, in minutes. If the automatic saving is disabled, this field is not displayed.
Filename	Filename of the saved configuration files, with path excluded.

display current-configuration

Syntax

display current-configuration [[**configuration** [*configuration*] | **interface** [*interface-type*] [*interface-number*] | **exclude** *modules*] [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]]

View

Any view

Default level

2: System level

Parameters

configuration [*configuration*]: Displays a non-interface configuration. If no parameter is used, all the non-interface configuration is displayed. If parameters are used, display the specified information. For example:

- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

interface [*interface-type*] [*interface-number*]: Displays the interface configuration, where *interface-type* represents the interface type and *interface-number* represents the interface number.

exclude *modules*: Excludes the configuration of the specified modules. The *modules* argument can be **acl**, **acl6**, or both separated by a space.

- **acl**: Excludes the IPv4 ACL configuration.
- **acl6**: Excludes the IPv6 ACL configuration.

by-linenum: Displays the number of each line.

|: Filters command output by specifying a regular expression. For more information about regular expressions, the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display current-configuration** to display the validated configuration of the switch.

A parameter is not displayed if it adopts the default configuration.

If the validated parameter is changed, it will be displayed. For example, IP address 11.11.11.11 24 has been configured on a Loopback interface. If you execute the **display current-configuration** command, IP address 11.11.11.11 255.255.255.255 is displayed, meaning the validated subnet mask is 32 bits.

Related commands: **display saved-configuration**, **reset saved-configuration**, and **save**.

Examples

# Display the configuration from the line containing "user-interface" to the last line in the current configuration.

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
user-interface vty 0 15
 authentication-mode none
 user privilege level 3
#
return
```

# Display the current SNMP configuration on the device.

```
<Sysname> display current-configuration | include snmp
 snmp-agent
 snmp-agent local-engineid 800063A203000FE240A1A6
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
```

display default-configuration

Syntax

display default-configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display default-configuration** to display the factory defaults of the device.

Related commands: **display current-configuration** and **display saved-configuration**.

Examples

# Display the factory defaults of the device. The factory defaults vary with switch models. The output is not shown here.

```
<Sysname> display default-configuration
```

display saved-configuration

Syntax

display saved-configuration [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

by-linenum: Identifies each line of displayed information with a line number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display saved-configuration** to display the contents of the saved startup configuration file.

During device management and maintenance, you can use this command to verify that important configurations are saved to the startup configuration file.

This command displays the main startup configuration file.

If the system is not specified with a startup configuration file or the specified configuration file does not exist, the **display saved-configuration** command displays the default configuration file of the device. If the default configuration file does not exist, the following message will appear "The config file does not exist!".

Related commands: **display current-configuration**, **reset saved-configuration,** and **save**.

Examples

# Display the saved startup configuration file.

```
<Sysname> display saved-configuration
#
 version 5.20, Test 5310
#
 sysname Sysname
#
 domain default enable system
#
 telnet server enable
#
 multicast routing-enable
#
 vlan 1
#
 vlan 999
#
 domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
 interface NULL0
#
  ---- More ----
```

The configurations are displayed in the order of global, port, and user interface. The More prompt indicates that there are more line that the screen can display. Pressing **Enter** displays the next line; pressing **Space** displays the next screen; pressing **Ctrl+C** or any other key exits the display.

# Display the contents of the saved startup configuration file with a number identifying each line.

```
<Sysname> display saved-configuration by-linenum
    1:  #
    2:   version 5.20, Test 5310
    3:  #
    4:   sysname Sysname
    5:  #
    6:   domain default enable system
    7:  #
    8:   telnet server enable
    9:  #
   10:   multicast routing-enable
   11:  #
   12:  vlan 1
   13:  #
   14:  vlan 999
   15:  #
   16:  domain system
   17:   access-limit disable
   18:   state active
   19:   idle-cut disable
   20:   self-service-url disable
   21:  #
   22:  interface NULL0
   23:  #
  ---- More ----
```

The More prompt indicates that there are more line that the screen can display. Pressing **Enter** displays the next line; pressing **Space** displays the next screen; pressing **Ctrl+C** or any other key exits the display.

display startup

Syntax

display startup [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display startup** to display the configuration files for the system startup and the configuration file(s) for the next system startup, and also the enabled/disabled status of the Boot ROM access control function if the function is supported on the device.

- The subordinate switches start and run based on the current configurations of the master. The startup configuration files displayed are always the same on all member switches of an IRF fabric.
- After the master is changed, the new master runs with the current configuration instead of restarting using the configuration file. When you execute the **display startup** command, the startup configuration file that is used for the current startup of the new master and subordinate switches is displayed as NULL.

Related commands: **startup saved-configuration**.

Examples

# Display the startup configuration file used at the current system startup and the startup configuration file(s) to be used at the next system startup.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: flash:/startup2.cfg
 Bootrom-access enable state: enabled
Slot 2:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: flash:/startup2.cfg
 Bootrom-access enable state: enabled
```

Table 12 Command output

Field	Description
MainBoard	Configuration files used at the current and the next startup of the master.
Current Startup saved-configuration file	Configuration file used at the current startup.
Next main startup saved-configuration file	Main configuration file used at the next startup.
Next backup startup saved-configuration file	Backup configuration file used at the next startup.

Field	Description
(This file does not exist.)	Indicates that the configuration file does not exist. If the user deletes the configuration file to be used at the next startup after configuring it, this message will be displayed after the filename.
Slot 2	Configuration files used at the current and the next startup of the subordinate switch (with the member ID 2).

display this

Syntax

display this [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

by-linenum: Displays the number of each line.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display this** to display the valid configuration information under the current view.

To check whether your configuration takes effect, use the **display this** command.

The valid configuration that adopts the default setting is not displayed.

The invalid configuration is not displayed.

Execution of this command in any user interface view displays the valid configuration in all the user interfaces.

Execution of this command in any VLAN view displays the configurations of all the created VLANs.

Examples

# Display the valid configuration information on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-Gigabitethernet1/0/1] display this
#
interface Gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 to 4 untagged
 port hybrid pvid vlan 2
#
return
```

# Display the valid configuration information of all user interfaces.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
user-interface aux 0
user-interface vty 0
 history-command max-size 256
user-interface vty 1 15
#
return
```

reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

Default level

3: Manage level

Parameters

backup: Deletes the backup startup configuration file.

main: Deletes the main startup configuration file.

Description

Use **reset saved-configuration** to delete the startup configuration file.

Delete the startup configuration file if it does not match the software version or has been corrupted.

This command permanently deletes the startup configuration file from all member switches of the IRF fabric. Use this command with caution.

You can choose to delete either the main or backup startup configuration file. If the main and backup startup configuration files are the same, if you perform the delete operation for once, the system will not delete the configuration file but only set the corresponding startup configuration file (main or backup) to NULL, and will not delete the configuration file.

If you execute either the **reset saved-configuration** command or the **reset saved-configuration main** command, the main startup configuration file will be deleted.

Related commands: **display saved-configuration** and **save**.

Examples

# Delete the startup configuration file from the storage media of the device.

```
<Sysname> reset saved-configuration backup
```

```
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash is being cleared.
Please wait ...
..
MainBoard:
 Configuration file is cleared.
Slot 2:
 Erase next configuration file successfully
```

restore startup-configuration

Syntax

restore startup-configuration from *src-addr src-filename*

View

User view

Default level

3: Manage level

Parameters

src-addr: IP address or name of a TFTP server. The address cannot be an IPv6 address.

src-filename: Filename of the configuration file to be downloaded from the specified server.

Description

Use **restore startup-configuration** to download a configuration file from the specified TFTP server to the device and specify it as the startup configuration file.

The file downloaded is set as the main startup configuration file.

This command downloads the configuration file to the root directory of the storage media of all the member switches and specifies the file as the startup configuration file of all the member switches.

If the file to be downloaded has the same filename as an existing file on a member switch, you will be prompted whether you want to overwrite the existing file or not.

Both the master and the subordinate switches are assumed to use the storage media of the same type when the device is checking the filename or backing up the configuration file to the subordinate switches. When backing up the configuration file to the subordinate switches, the device saves the file to the same directory on the subordinate switches as on the master, that is, the root directory.

Examples

# Download file **config.cfg** from the TFTP server at 2.2.2.2, and specify the file as the main startup configuration file of the device.

```
<Sysname> restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...finished!
Now restore next startup-configuration file from main to slave board. Please
wait...finished!
```

save

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**]

View

Any view

Default level

2: System level

Parameters

file-url: File path, where the extension of the file name must be .cfg. When used with the keyword **all** or **slot**, this argument cannot include a member ID. If the file path includes a folder name, you must first create the folder on the member switch.

all: Saves the current configuration with the specified filename to all member switches of an IRF fabric.

slot *slot-number*: Saves the current configuration with the specified filename to a subordinate switch. *slot-number* represents the member ID of a member switch of an IRF fabric.

safely: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

backup: Saves the current configuration to the startup configuration file specified in the interactive mode, and specifies the file as the backup startup configuration file of the device.

main: Saves the current configuration to the main startup configuration file specified in the interactive mode, and specifies the file as the main startup configuration file of the device.

force: Saves the current configuration to the startup configuration file of the device, and the system does not output any interaction information. By default, when you execute the **save** command, the system asks you to input **Y** or **N** to confirm your operation. If you do not confirm your operation within 30 seconds, the system automatically quits the operation. If you provide the **force** keyword when executing the **save** command, the system directly saves the current configuration, not requiring any confirmation.

Description

Use **save** *file-url* [**all** | **slot** *slot-number*] to save the current configuration to the specified configuration file, but the system does not specify the file as the startup configuration file. If the file specified by *file-url* does not exist, the system creates the file and then saves the configuration to the file; if the **all** or **slot** keyword is not specified, the configuration is saved to the master.

Use **save** [**safely**] [**backup** | **main**] [**force**] to save the current configuration to the root directory of the storage media on a member switch, and specify the file as the startup configuration file. If the **backup** or **main** keyword is not specified, the **main** keyword is used by default.

Whether the **save** [**safely**] [**backup** | **main**] [**force**] command or the **save** *file-url* **all** command+**Enter** takes effect on all the member switches or only on the master depends on whether the configuration file auto-save function is enabled.

Related commands: **display current-configuration**, **display saved-configuration**, **reset saved-configuration**, and **slave auto-update config**.

Examples

# Save the current configuration to the root directory of the storage media on a member switch, and specify the file as the startup configuration file.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/aa.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/aa.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled
```

*// The above information indicates that the main startup configuration file of all the member switches is **aa.cfg**.*

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/aa.cfg]
(To leave the existing filename unchanged, press the enter key):startup.cfg
flash:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait.................
 The current configuration is saved to the active main board successfully.
Slot 2:
 The current configuration file is saved successfully.
 Configuration is saved to device successfully.
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled
```

*// The above information indicates that the main startup configuration file of all member switches of the IRF fabric is changed to **startup.cfg**.*

# Save the current configuration in the name of **test.cfg** to a subordinate switch (with the member ID of 2) (approach 1).

```
<Sysname> save test.cfg slot 2
The current configuration will be saved to slot2#flash:/test.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration slot2#flash:/test.cfg. Please wait...
.........
Configuration is saved to slot2#flash successfully.
```

Or, you can use the following command (approach 2):

```
<Sysname> save slot2#flash:/test.cfg
```

# Save the current configuration to the startup configuration file of the device, without any confirmation required.

```
<Sysname> save force
 Validating file. Please wait.................
 The current configuration is saved to the active main board successfully.
Slot 2:
 The current configuration file is saved successfully.
 Configuration is saved to device successfully.
```

slave auto-update config

Syntax

slave auto-update config

undo slave auto-update config

View

System view

Default level

2: System level

Parameters

None

Description

Use **slave auto-update config** to enable the configuration file auto-save function.

Use **undo slave auto-update config** to disable the function.

By default, the configuration file auto-save function is enabled.

NOTE:

This function is only available on switches that support IRF.

Examples

# Enable the configuration file auto-save function.

```
<Sysname> system-view
[Sysname] slave auto-update config
```

startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

View

User view

Default level

3: Manage level

Parameters

cfgfile: Configuration file name. The file must be a file with an extension .cfg stored in the storage media's root directory.

backup: Sets the configuration file as the backup startup configuration file of the device.

main: Sets the configuration file as the main startup configuration file of the device.

Description

Use **startup saved-configuration** to specify a startup configuration file for all the member switches.

Use **undo startup saved-configuration** to configure all the member switches to start up with the null configuration (the factory configuration).

The startup configuration files of all the member switches must be the same. Therefore, before using the command, make sure that the specified configuration file has been saved to the root directories of the storage media of all the member switches; otherwise, the command will fail.

When you execute the **undo startup saved-configuration** command and reboot the IRF fabric or an IRF member switch, the IRF fabric is partitioned. Therefore, use this command with caution.

When a device supports **main**/**backup** keyword:

- Both the **startup saved-configuration** and **startup saved-configuration main** commands can be used to specify the main startup configuration file.
- The main and backup startup configuration files can be specified as the same file. However, it is recommended you use different files, or, save the same configuration as two files using different file names, one specified as the main startup configuration file, and the other specified as the backup.
- If you execute the **undo startup saved-configuration** command, the system sets the main and backup startup configuration files as NULL, but does not delete the two configuration files.

Related commands: **display startup**.

Examples

# Specify a startup configuration file.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ...
Setting the master board ..........
... Done!
Setting the slave board ...
Slot 2:
 Set next configuration file successfully
```

Software upgrade commands

boot-loader

Syntax

boot-loader file *file-url* **slot** { **all** | *slot-number* } { **main** | **backup** }

View

User view

Default level

3: Manage level

Parameters

file *file-url*: Specifies a file name, a string of 1 to 63 characters. If you enter a relative path here, the system automatically converts it to an absolute path. The absolute path should contain no more than 63 characters. The file name is in the format [*drive*:/]*file-name*, where

- The items in square brackets [ ] are optional.
- *drive* specifies the storage media of the file. The value is the name of the storage media. If a switch has only one storage media, you can execute this command without providing this argument.
- *file-name* specifies the filename, which is usually has the **.app** or **.bin** suffix.

slot *slot-number*: Specifies the member ID of a device.

- **all**: Specifies a file as the system software image at the next boot for all member switches of an IRF fabric.
- *slot-number*: Specifies a file as the system software image at the next boot for a member switch. The *slot-number* argument is the ID of a member switch of the current IRF fabric.

main: Specifies a file as the main system software image. A main system software image is used to boot a device.

backup: Specifies a file as a backup system software image. A backup system software image is used to boot a device only when a main system software image is unavailable.

Description

Use **boot-loader** to specify the system software image for the next boot of a member switch.

To execute the **boot-loader** command successfully, save the file for the next device boot in the root directory of the storage media on a member switch.

If the storage media is on the master, you can specify the storage media by giving its name, such as **flash**; if the storage media is on a subordinate switch, you can specify the storage media by giving its name and the member ID of the device, in the format of slot*slot-number# StorageMediumName*, where *slot-number* represents the member ID of the salve, such as **slot2#flash**.

When you specify the system software image of the master, the *file-url* argument cannot contain the member ID of the device, and *slot-number* should be specified as the member ID of the master; when you specify the system software image of the subordinate switch, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), and *slot-number* should be specified as the member ID of the subordinate switch.

If you provide the keyword **all**, the *file-url* argument cannot contain a member ID, otherwise, the execution of this command will fail; you must save the specified system software image on the storage media of all member switches in the same filename or the file will fail to be reconfigured during the reboot.

The names of the files for the next boot of the master and subordinate switches may be different, but the versions of the files must be the same, or a subordinate switch will reboot by using the master's system software image and join the IRF fabric again.

Related commands: **display boot-loader**.

Examples

# Specify the main system software image for the master (the member ID is 1) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage media of the master. Otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file test.bin slot 1 main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 1!
```

# Specify the main system software image for the subordinate switch (the member ID is 2) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage media of the subordinate switch. Otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file slot2#flash:/test.bin slot 2 main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 2!
```

# Specify the main system software image for all member switches for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage media of all the member switches. Otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file test.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

boot-loader update file

Syntax

boot-loader update file *file-url* **slot** { *slot-number* | **all** } { **main** | **backup** }

View

User view

Default level

3: Manage level

Parameters

file-url: Specifies a file name, a string of 1 to 63 characters. For more information, see boot-loader.

slot: Specifies the member ID of a device.

- *slot-number*: Specifies to upgrade the system software image of a member switch. *slot-number* is the ID of a member switch of the current IRF fabric.
- **all**: Specifies to upgrade system software images for or all member switches of an IRF fabric.

main: Specifies a file as the main system software image. A main system software image is used to boot a device.

backup: Specifies a file as the backup system software image. A backup system software image is used to boot a device only when a main system software image is unavailable.

Description

Use **boot-loader update file** to specify the system software image for the next boot of a specified member switch or all the member switches of an IRF fabric.

Execution of this command equals the following two steps

Copy a system software image to a specified IRF member switch. If the **all** keyword is specified, the system software image is copied to all the member switches of the current IRF fabric.

Specify the file as the system software image to be used at the next boot of the member switch.

NOTE:

The command is applicable to IRF-supported switches.

Examples

# Specify the system software image for the next boot of all member switches of an IRF fabric.

```
<Sysname> tftp 192.168.1.26 get main.bin
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP: 10105088 bytes received in 36 second(s)
  File downloaded successfully.
<Sysname> boot-loader update file main.bin slot all main
This command will update the specified boot file of all boards. Continue? [Y/N]:Y
Now is updating, please wait...
<Sysname> reboot
```

bootrom

Syntax

bootrom update file *file-url* **slot** *slot-number-list*

View

User view

Default level

3: Manage level

Parameters

update file *file-url*: Upgrades Boot ROM, *where file-url* is a string of 1 to 63 characters and represents the name of the file to be upgraded.

slot *slot-number-list*: Specifies a list of IDs of member switches, in the format of { *slot-number* [**to** *slot-number*] }&<1-7>. The *slot-number* argument is the ID of an IRF member switch to be upgraded.

Description

Use **bootrom** to upgrade Boot ROM on member switches.

To upgrade Boot ROM for an IRF member switch, first save the corresponding Boot ROM image under the root directory of the storage media on the master.

When you upgrade Boot ROM for the master, the *file-url* argument cannot contain the member ID of the device.

When you upgrade Boot ROM for a subordinate switch, if the Boot ROM image is already saved under the root directory of the storage media on this subordinate switch, the *file-url* argument can contain the member ID (such as **slot2#flash:/test.bin**). Otherwise, the *file-url* argument cannot contain the member ID.

Use **bootrom** to upgrade Boot ROM on member switches.

To upgrade Boot ROM for an IRF member switch, first save the corresponding Boot ROM image under the root directory of the storage media on the member switch.

When you upgrade Boot ROM for the master, the *file-url* argument cannot contain the member ID of the device.

When you upgrade Boot ROM for a subordinate switch, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), *slot-number* should be specified as the member ID of the subordinate switch.

Examples

# Use the **a.btm** file to upgrade Boot ROM on the master with member ID of 1.

```
<Sysname> bootrom update file a.btm slot 1
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  Now updating bootrom, please wait...
  Bootrom update succeeded in slot 1.
```

# Use the **a.btm** file to upgrade Boot ROM on the subordinate switch with member ID of 2. The **a.btm** file is saved under the root directory of the storage medium on the subordinate switch.

```
<Sysname> bootrom update file slot2#flash:/a.btm slot 2
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  Now updating bootrom, please wait...
  Bootrom update succeeded in slot 2.
```

bootrom-update security-check enable

Syntax

bootrom-update security-check enable

undo bootrom-update security-check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **bootrom-update security-check enable** to enable the validity check function when upgrading Boot ROM.

Use **undo bootrom-update security-check enable** to disable the validity check function when upgrading Boot ROM.

By default, the validity check function is enabled when Boot ROM is upgrading.

When the validity check function is enabled, the switch will strictly check whether the Boot ROM upgrade files are valid and can match the hardware.

Examples

# Enable the validity check function when upgrading Boot ROM.

```
<Sysname> system-view
[Sysname] bootrom-update security-check enable
```

display boot-loader

Syntax

display boot-loader [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Displays system software information of a member switch. The *slot-number* argument is the ID of a member switch of the current IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display boot-loader** to display information about the system software.

Related commands: **boot-loader**.

Examples

# Display the file adopted for the current and next boot of the device.

```
<Sysname> display boot-loader
 Slot 1
The current boot app is:  flash:/test.bin
The main boot app is:     flash:/test.bin
The backup boot app is:   flash:/test.bin
```

Table 13 Command output

Field	Description
Slot 1	The member ID of the device is 1.
The current boot app is	System software image used for the device for the current device boot.

Field	Description
The main boot app is	Main system software image used for the next device boot of the device.
The backup boot app is	Backup system software image used for the next device boot of the device.

display patch

Syntax

display patch [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display patch** to display the installed patch files and the versions of their corresponding patch packages. If a patch is not loaded from a patch package, the version of the patch package is not displayed.

Examples

# Display the installed patch files and the versions of their corresponding patch packages.

```
<Sysname> display patch
The following patch packages are loaded:
flash:/patch-package.bin, Package-Version-001, loaded on slot(s):
1
```

Table 14 Command output

Field	Description
flash:/patch-package.bin	Directory of the installed patch file.
Package-Version-001	Version of the patch package.
loaded on slot(s):	Slot number of the IRF member switch on which the patch loaded.

display patch information

Syntax

display patch information [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display patch information** to display the hotfix information.

Examples

# Display hotfix information.

```
<Sysname> display patch information
The location of patches: flash:/
Slot Version   Temporary Common Current Active Running  Start-Address
----------------------------------------------------------------------
1    XXX        0           0       0        0        0         0x53f8364
```

Table 15 Command output

Field	Description
The location of patches	Patch file location. You can configure it using the **patch location** command.
Slot	Member ID.
Version	Patch version.
Temporary	Number of temporary patches.
Common	Number of common patches.
Current	Total number of patches.
Running	Number of patches in RUNNING state.
Active	Number of patches in ACTIVE state.
Start-Address	Starting address of the memory patch area in the memory.

patch active

Syntax

patch active [*patch-number*] **slot** *slot-number*

View

System view

Default level

3: Manage level

Parameters

patch-number: Sequence number of a patch, with values depending on the patch file used.

slot *slot-number*: Specifies the ID of a member switch of the current IRF fabric.

Description

Use **patch active** to activate patches. The system will temporarily run the loaded patches.

If you execute the command with specifying the sequence number of a patch, all the DEACTIVE patches (including the specified patch) before the specified patch will be activated.

If you execute the command without specifying the sequence number of a patch, all the DEACTIVE patches will be activated.

This command is applicable to only patches in DEACTIVE state.

After a system reboot, the original ACTIVE patches change to DEACTIVE and become invalid. To make them effective, activate them again.

Examples

# Activate patch 3 and all the loaded DEACTIVE patches before patch 3 on the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch active 3 slot 1
```

# Activate all the loaded patches on the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch active slot 1
```

patch deactive

Syntax

patch deactive [*patch-number*] **slot** *slot-number*

View

System view

Default level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies the ID of a member switch of the current IRF fabric.

Description

Use **patch deactive** to stop running patches and the system will run at the original software version.

If you execute the command with specifying the sequence number of a patch, all the ACTIVE patches (including the specified patch) after the specified patch turn to DEACTIVE state.

If you execute the command without specifying the sequence number of a patch, all the ACTIVE patches turn to DEACTIVE state.

This command is not applicable to the patches in RUNNING state.

Examples

# Stop running patch 3 and all the ACTIVE patches after patch 3 on the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch deactive 3 slot 1
```

# Stop running all the ACTIVE patches on the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch deactive slot 1
```

patch delete

Syntax

patch delete [*patch-number*] **slot** *slot-number*

View

System view

Default level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies the ID of a member switch of the current IRF fabric.

Description

Use **patch delete** to delete patches and all the patches after the specified patch.

If you execute the command with specifying the sequence number of a patch, all the patches (including the specified patch) after the specified patch will be deleted.

If you execute the command without specifying the sequence number of a patch, all the patches will be deleted.

This command only removes the patches from the memory patch area, and it does not delete them from the storage media. The patches are in IDLE state after this command is executed.

Examples

# Delete patch 3 and all the patches after patch 3 on the IRF member switch with member ID 1.

```
<Sysname> system-view
[Sysname] patch delete 3 slot 1
```

# Delete patch 3 and all the patches after patch 3 on the IRF member switch with member ID 1.

```
<Sysname> system-view
[Sysname] patch delete slot 1
```

patch install

Syntax

patch install { *patch-location* | **file** *filename* }

undo patch install

View

System view

Default level

3: Manage level

Parameters

patch-location: A string consisting of 1 to 64 characters. It specifies the directory where the patch file locates and must be a root directory of a storage media. Provide this argument when you install a patch file which is not packaged in a patch package file. The provided patch file name must be valid. Otherwise, the system cannot locate the patch file and the hotfixing operation fails.

file *filename*: Filename of a patch package. Provide this option when you install a patch package file, which contains multiple patches released at the same time.

Description

Use **patch install** to install all the patches in one step.

Use **undo patch install** to remove the patches.

When you execute the **patch install** command, message "Do you want to continue running patches after reboot? [Y/N]:" is displayed.

- Entering **y** or **Y**: All the specified patches are installed, and turn to RUNNING state from IDLE. This equals execution of the commands **patch location**, **patch load**, **patch active**, and **patch run**. The patches remain RUNNING after system reboot. If a slot is empty, the system will record the information.
- Entering **n** or **N**: All the specified patches are installed and turn to ACTIVE state from IDLE. This equals execution of the commands **patch location**, **patch load** and **patch active**. The patches turn to DEACTIVE state after system reboot.

Before executing the command, save patch files to the specified directory. Follow these rules:

- Before installing patches, save the patch package file or patch files to root directories of the storage media on all member switches.

Examples

# Install the patches located on the Flash.

```
<Sysname> system-view
[Sysname] patch install flash:
Patches will be installed. Continue? [Y/N]:y
Do you want to run patches after reboot? [Y/N]:y
Installing patches…
```

# Install the specified patch package.

```
<Sysname> system-view
[Sysname] patch install file:/patch_package.bin
Patches will be installed. Continue? [Y/N]:y
Do you want to run patches after reboot? [Y/N]:y
Installing patches…
```

patch load

Syntax

patch load slot *slot-number* [**file** *filename*]

View

System view

Default level

3: Manage level

Parameters

slot *slot-number*: Specifies the ID of a member switch of the current IRF fabric.

file *filename*: Filename of a patch package.

Description

Use **patch load** to load the patch file on the storage media (the Flash) to the memory patch area.

If you execute the command with providing the filename of a patch package, the system will load the patch from the patch package. If you execute the command without providing the filename of a patch package, the system will load the patch from a patch file.

The system loads the patch file from the Flash by default.

Before executing the command, save the patch files to the specified directory. The following rules apply:

- Before loading patches, save the patch package file or patch files to root directories of the storage media on all member switches.

Examples

# Load the patch file from a patch file for the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch load slot 1
```

# Load the patch file from a patch package for the IRF member switch with member ID of 1.

```
<Sysname> system-view
[Sysname] patch load slot 1 file flash:/patchpackage.bin
```

patch location

Syntax

patch location *patch-location*

View

System view

Default level

3: Manage level

Parameters

patch-location: Specifies the patch file location, a string of 1 to 64 characters. It can be a root directory of a storage media.

Description

Use **patch location** to configure the patch file location.

By default, the patch file location is **flash:**.

If you want to install a patch package, you do not need to configure this command.

Examples

# Configure the root directory of the Flash as the patch file location.

```
<Sysname> system-view
[Sysname] patch location flash:
```

patch run

Syntax

patch run [*patch-number*] [**slot** *slot-number*]

View

System view

Default level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies the ID of a member switch of the current IRF fabric.

Description

Use **patch run** to confirm the running of ACTIVE patches.

If you execute the command with specifying the sequence number of a patch, the command confirms the running of all the ACTIVE patches (including the specified patch) before the specified patch. If you execute the command without specifying the sequence number of a patch, the command confirms the running of all the ACTIVE patches.

This command is applicable to patches in ACTIVE state only.

If the running of a patch is confirmed, the patch will still be effective after the system reboots.

Examples

# Confirm the running of patch 3 and all the ACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch run 3 slot 1
```

# Confirm the running all the ACTIVE patches on the IRF member switch with member ID 1.

```
<Sysname> system-view
[Sysname] patch run slot 1
```

Device management commands

brand

Syntax

brand { **hp** | **h3c** } [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch. If this option is not specified, the command applies to all member switches in the IRF fabric.

Description

Use **brand** to change the brand name for an IRF member switch.

After you perform this command, use the **display brand** command to verify the new brand name and then reboot the member switch to make your change take effect.

Examples

# Display brand information.

```
<HP>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
<HP>
```

# Change the brand name of member switch 3 to HP.

```
<HP>brand hp slot 3
Configuration will take effect after next reboot.
 Do you want to continue? [Y/N]:y
 Configuration is successful.
```

# Display brand information.

```
<HP>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: HP.
```

```
<HP>
```

The output shows that the brand name has been changed. After a reboot, member switch 3 becomes an HP member switch.

clock datetime

Syntax

clock datetime *time date*

View

User view

Default level

3: Manage level

Parameters

time: Specifies a time, in the *hh:mm:ss* format. The *hh* value ranges from 00 to 23, the *mm* value ranges from 00 to 59, and the *ss* value ranges from 00 to 59. Zeros can be omitted, unless you specify 00:00:00.

date: Specifies a date, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value ranges from 1 to 31.

Description

Use **clock datetime** to set the system time and date.

You can leave the *ss* field blank when you specify the time parameters.

Related commands: **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**, and **display clock**.

Examples

# Set the current system time to 14:10:20 08/01/2011.

```
<Sysname> clock datetime 14:10:20 8/1/2011
```

# Set the current system time to 00:06:00 01/01/2011.

```
<Sysname> clock datetime 0:6 2011/1/1
```

clock summer-time one-off

Syntax

clock summer-time *zone-name* **one-off** *start-time start-date end-time end-date add-time*

undo clock summer-time

View

System view

Default level

3: Manage level

Parameters

zone-name: Specifies a daylight saving time by its zone name, a case-sensitive string of 1 to 32 characters.

start-time: Start time, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

start-date: Start date, in the *MM/DD/YYYY* or *YYYY/MM/DD* format.

end-time: End time, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

end-date: End date, in the *MM/DD/YYYY* or *YYYY/MM/DD* format.

add-time: Time added to the standard time of the device, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

Description

Use **clock summer-time one-off** to adopt daylight saving time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Daylight saving time adds the *add-time* to the standard time of the device.

Use **undo clock summer-time** to cancel the configuration of the daylight saving time.

By default, daylight saving time is disabled and the UTC time zone applies.

The interval between *start-time start-date* and *end-time end-date* must be longer than one day and shorter than one year. If the current system time is in the specified daylight saving days, the *add-time* value automatically adds to the system time.

To verify the setting, use the **display clock** command.

The timestamps in system messages are adjusted in reference to the time zone and daylight saving schedule.

Related commands: **clock datetime**, **clock summer-time repeating**, **clock timezone**, and **display clock**.

Examples

# Set the system time ahead one hour for the period between 06:00:00 on 08/01/2011 and 06:00:00 on 09/01/2011.

```
<Sysname> system-view
[Sysname] clock summer-time abc1 one-off 6 08/01/2011 6 09/01/2011 1
```

clock summer-time repeating

Syntax

clock summer-time *zone-name* **repeating** *start-time start-date end-time end-date add-time*

undo clock summer-time

View

System view

Default level

3: Manage level

Parameters

zone-name: Name of the daylight saving time, which is a string of 1 to 32 characters.

start-time: Start time, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

start-date: Start date, which can be set in the following ways:

- Enter the year, month and date at one time, in the *MM/DD/YYYY* or *YYYY/MM/DD* format.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**,

October, **November** or **December**; the start week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the start date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

end-time: End time, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

end-date: End date which can be set in the following ways:

- Enter the year, month and date at one time, in the *MM/DD/YYYY* or *YYYY/MM/DD* format.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the end week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the end date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

add-time: Time added to the standard time of the device, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

Description

Use **clock summer-time repeating** to set a recurring daylight saving schedule.

Use **undo clock summer-time** to cancel the configuration of the daylight saving time.

By default, daylight saving time is disabled and UTC time zone applies.

The interval between *start-time start-date* and *end-time end-date* must be longer than one day and shorter than one year. If the current system time is in the specified daylight saving days, the *add-time* value automatically adds to the system time.

To verify the setting, use the **display clock** command.

The timestamps in system messages are adjusted in reference to the time zone and daylight saving schedule.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock timezone**, and **display clock**.

Examples

# Set the system time ahead one hour every year after 2011 (inclusive) for the period from August 1 at 06:00:00 to September 1 at 06:00:00.

```
<Sysname> system-view
[Sysname] clock summer-time abc2 repeating 06:00:00 08/01/2011 06:00:00 09/01/2011
01:00:00
```

clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

View

System view

Default level

3: Manage level

Parameters

zone-name: Specifies a time zone by its name, a case-sensitive string of 1 to 32 characters.

add: Adds a specified offset to UTC time.

minus: Subtracts a specified offset to UTC time.

zone-offset: Specifies an offset to the UTC time, in the *hh:mm:ss* format. Zeros can be omitted, unless you specify 00:00:00.

Description

Use **clock timezone** to set the local time zone.

Use **undo clock timezone** to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

To verify the setting, use the **display clock** command.

The timestamps in system messages are adjusted in reference to the time zone and daylight saving schedule.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, and **display clock**.

Examples

# Set the local time zone to add five hours to UTC time.

```
<Sysname> system-view
[Sysname] clock timezone z5 add 5
```

copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **copyright-info enable** to enable displaying the copyright statement.

Use **undo copyright-info enable** to disable displaying the copyright statement.

By default, this feature is enabled.

Examples

# Enable displaying the copyright statement.

```
<Sysname> system-view
[Sysname] copyright-info enable
```

- When a Telnet user logs in, the following statement appears:

  ```
  ****************************************************************************
  * Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.        *
  ```

```
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
****************************************************************************
<Sysname>
```

- When a console user quits user view, the following statement appears:

```
****************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.        *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
****************************************************************************
User interface aux0 is available.



Please press ENTER.
```

# Disable displaying the copyright statement.

```
<Sysname> system-view
[Sysname] undo copyright-info enable
```

- When a Telnet user logs in, the user view prompt appears:

```
<Sysname>
```

- When a console user quits user view, the following message appears:

```
User interface aux0 is available.



Please press ENTER.
```

display alarm

Syntax

display alarm [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays alarms presents on an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, this command displays alarm information for all IRF member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display alarm** to display device alarms.

Examples

# Display device alarms.

```
<Sysname> display alarm
Slot  Level    Info
6     ERROR    Fan 2 is absent.
6     ERROR    Power 2 is absent.
6     ERROR    The board in slot 10 is faulty.
3     WARNING  The temperature of sensor 3 exceeds the lower limit.
```

Table 16 Command output

Field	Description
Slot	ID of the alarming device
Level	Alarm severity level, including ERROR, WARNING, NOTICE, and INFO in descending order
Info	Detailed alarm information

display brand

Syntax

display brand [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

User view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display brand** to display the brand name of a member switch.

Examples

# Display the brand name of the current member switch.

```
<HP>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
<HP>
```

display clock

Syntax

display clock [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display clock** to display the system time and date.

The system time and date are decided by the **clock datetime**, **clock summer-time one-off** (or **clock summer-time repeating**), and **clock timezone** commands. For more information about how the system time and date are decided, see *Fundamentals Configuration Guide*.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, and **clock timezone**.

Examples

# Display the current time and date.

```
<Sysname> display clock
09:41:23 UTC Thu 12/15/2010
```

display cpu-usage

Syntax

display cpu-usage [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display cpu-usage *entry-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Number of entries to be displayed, which ranges from 1 to 60.

offset: Offset between the serial number of the first CPU usage rate record to be displayed and that of the last CPU usage rate record to be displayed. It ranges from 0 to 59.

For example, the idx of the latest statistics record is 12. If the *offset* is set to 3, the system will display the statistics records from the one with the idx of 9, where idx represents the serial number of the period for the statistics, and its value ranges from 0 to 60 cyclically. The system collects CPU usage rates periodically, and the system records the average CPU usage rate during this period, and the idx value is added by 1 automatically.

verbose: Displays the average CPU usage statistics for each task in the specified period. If this keyword is not provided, the system displays brief CPU usage statistics.

slot *slot-number*: Displays the CPU usage statistics for an IRF member switches. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, the system displays the CPU usage statistics for all IRF member switches.

cpu *cpu-number*: Displays the CPU usage statistics for the specified CPU. If the *cpu-number* argument is not provided, the system displays the CPU usage statistics for all CPUs of the specified IRF member switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cpu-usage** to display CPU usage statistics.

The system regularly (typically at 60-second intervals) collects CPU usage statistics and saves the statistical results in the history record area.

The **display cpu-usage** *entry-number* command displays *entry-number* latest records, starting from the latest record. The **display cpu-usage** *entry-number offset* command displays *entry-number* latest records, starting from the last (*offset*+1)th record.

Examples

# Display the current CPU usage statistics.

```
<Sysname> display cpu-usage
Slot 1 CPU usage:
       9% in last 5 seconds
       8% in last 1 minute
       8% in last 5 minutes
```

# Display the last fifth and sixth CPU usage statistics records.

```
<Sysname> display cpu-usage 2 4
===== CPU usage info (no:  0  idx: 58) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2010-07-10  10:56:55
CPU Usage Stat. Tick : 0x1d9d(CPU Tick High) 0x3a659a70(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x95030517(CPU Tick Low)

===== CPU usage info (no:  1  idx: 57) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2010-07-10  10:55:55
CPU Usage Stat. Tick : 0x1d9c(CPU Tick High) 0xa50e5351(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x950906af(CPU Tick Low)
```

Table 17 Command output

Field	Description
Slot 1	CPU usage statistics for the device (whose member ID is 1).
1% in last 5 seconds	After a boot, the system calculates and records the average CPU usage rate every five seconds. This field displays the average CPU usage rate in the last five seconds.
1% in last 1 minute	After a boot, the system calculates and records the average CPU usage rate every one minute. This field displays the average CPU usage rate in the last minute.
1% in last 5 minutes	After a boot, the system calculates and records the average CPU usage rate every five minutes. This field displays the average CPU usage rate in the last five minutes.
CPU usage info (no: idx:)	Information of CPU usage rate records (no: The (no+1)th record is displayed. no numbers from 0, a smaller number equals a newer record. idx: index of the current record in the history record table). If only the information of the current record is displayed, no and idx are not displayed.
CPU Usage Stat. Cycle	CPU usage rate measurement interval, in seconds. For example, if the value is 41, it indicates that the average CPU usage rate during the last 41 seconds is calculated. The value range of this field is 1 to 60.
CPU Usage	Average CPU usage rate in a measurement interval, in percentage.
CPU Usage Stat. Time	CPU usage rate statistics time in seconds, that is, the system time when the command is executed.
CPU Usage Stat. Tick	System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits.
Actual Stat. Cycle	Actual CPU usage rate measurement interval in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage rate records might differ slightly.

display cpu-usage history

Syntax

display cpu-usage history [**task** *task-id*] [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

task *task-id*: Displays the historical CPU usage statistics for the specified task, where *task-id* represents the task number. If no task is specified, the system displays the historical CPU usage statistics for the entire system (the CPU usage statistics for the entire system is the sum of CPU usage statistics for all tasks).

slot *slot-number*: Displays the historical CPU usage statistics for an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, the system displays the historical CPU usage statistics for the master.

cpu *cpu-number*: Displays the historical CPU usage statistics for the specified CPU. If the *cpu-number* argument is not provided, the system displays the historical CPU usage statistics for the main CPU.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cpu-usage history** to display historical CPU usage statistics in a chart.

The system regularly collects CPU usage statistics and saves the statistics in the history record area. The **display cpu-usage history** command displays the CPU usage statistics for the last 60 minutes in axes, where:

- The vertical axis represents the CPU usage. If a statistic is not a multiple of the usage step, it is rounded up or down to the closest multiple of the usage step, whichever is closer. For example, if the CPU usage step is 5%, the statistic 53% is rounded up to 55%, and the statistic 52% is rounded down to 50%.
- The horizontal axis represents the time.
- Consecutive pound signs (#) indicate the CPU usage at a specific time. The value on the vertical axis for the topmost # sign at a specific time represents the CPU usage at that time.

Examples

# Display historical CPU usage statistics.

```
<Sysname> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|             #
 10%|            ###  #
  5%|           ########
     ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
                      cpu-usage last 60 minutes(SYSTEM)
```

The output shows the historical CPU usage statistics (with the task name **SYSTEM**) in the last 60 minutes:

- 5%: 12 minutes ago
- 10%: 13 minutes ago
- 15%: 14 minutes ago
- 10%: 15 minutes ago
- 5%: 16 and 17 minutes ago
- 10%: 18 minutes ago
- 5%: 19 minutes ago
- 2% or lower than 2%: other time

# Display the historical CPU usage statistics of task 6.

```
<Sysname> display cpu-usage history task 6
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|                   #
     ------------------------------------------------------------
              10        20        30        40        50        60   (minutes)
                      cpu-usage last 60 minutes(T03M)
```

The output shows the historical CPU usage statistics of task 6 (with the task name **T03M**) in the last 60 minutes:

- 5%: 20 minutes ago
- 2% or lower than 2%: other time

display device

Syntax

display device [[**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Displays information about an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

subslot *subslot-number*: Displays information about the specified host or subcard (interface card). The *subslot-number* represents the subslot of the host or subcard. If the switch does not support the subcard or the subcard is not installed, 0 is displayed.

verbose: Displays detailed information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display device** to display device information.

Examples

# Display device information.

```
<Sysname>display device
Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
```

```
0      52      REV.B  NULL    007     607        IVL    MAIN       Normal
```

Table 18 Command output

Field	Description
Slot 1	Information about the device (whose member ID is 1)
SubSNo	Number of the slot in which the host or subcard resides
PortNum	Maximum number of ports that the host or subcard supports
PCBVer	PCB version of the host or subcard
FPGAVer	FPGA version of the host or subcard
CPLDVer	CPLD version of the host or subcard
BootRomVer	Boot ROM version of the host or subcard
AddrLM	Address learning mode: • IVL: Independent VLAN learning • SVL: Shared VLAN learning
Type	Type of the host or subcard: • Host: MAIN is displayed for this type • Subcard: The specific model is displayed for this type
State	State of the host or subcard: • Normal • Absent • Fault

display device manuinfo

Syntax

display device manuinfo [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

slot *slot-number*: Displays the electronic label data for an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, the system displays the electronic label data for all IRF member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display device manuinfo** to display electronic label data.

An electronic label is a profile of a device or card and contains the permanent configuration including the serial number, manufacturing date, MAC address, and vendor name. The data is written to the storage component during debugging or testing.

Examples

# Display electronic label data.

```
<Sysname> display device manuinfo
Slot 1:
DEVICE_NAME          : HP 5120-48G-PoE+ EI Switch with 2 Interface Slots JG237A
DEVICE_SERIAL_NUMBER : 210235A04TH08A000161
MAC_ADDRESS          : 000F-E2D2-58FB
MANUFACTURING_DATE   : 2008-11-08
VENDOR_NAME          : HP
```

Table 19 Command output

Field	Description
Slot	Device ID
DEVICE_NAME	Device name
DEVICE_SERIAL_NUMBER	Device serial number
MAC_ADDRESS	MAC address of the device
MANUFACTURING_DATE	Manufacturing date of the device
VENDOR_NAME	Vendor name

display diagnostic-information

Syntax

display diagnostic-information [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display diagnostic-information** to display or save operating statistics for multiple feature modules in the system.

For diagnosis or troubleshooting, you can use separate **display** commands to collect running status data module by module, or use the **display diagnostic-information** command to bulk collect running data for multiple modules. The **display diagnostic-information** command equals this set of commands: **display clock**, **display version**, **display device**, and **display current-configuration**.

Examples

# Save each module's running status data.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

To view the content of file **aa.diag**, execute the **more.aa.diag** command in user view, in combination of the **Page Up** and **Page Down** keys.

# Display the operating statistics for multiple feature modules in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
=================================================
  ===============display clock===============
=================================================
08:54:16 UTC Fri 11/15/2010
===================================================
  ===============display version===============
===================================================
```

…Part of the output is not shown…

display environment

Syntax

display environment [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays temperature information for an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display environment** to display temperature information, including the current temperature and thresholds.

If no member switch is specified, this command display temperature information for all member switches.

Related commands: **temperature-limit**.

Examples

# Display temperature information.

```
<Sysname> display environment
Slot 1
System temperature information (degree centigrade):
---------------------------------------------------------------------------
Sensor     Temperature  LowerLimit  WarningLimit  AlarmLimit ShutdownLimit
hotspot 1  28           -5          55            NA          NA
```

Table 20 Command output

Field	Description
Slot	Device ID.
sensor	Temperature sensor: hotspot: A hotspot sensor.
Temperature	Current temperature.
LowerLimit	Lower temperature threshold.
WarningLimit	Warning temperature threshold.
AlarmLimit	Alarming temperature threshold.
ShutdownLimit	Shutdown temperature threshold. When the sensor temperature reaches this limit, the system shuts down automatically.

display fan

Syntax

display fan [**slot** *slot-number* [*fan-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the operating state of fan trays for an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, the system displays the operating state of fan trays for all IRF member switches.

fan-id: Displays the operating state of the specified fan tray, where *fan-id* represents the fan tray number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display fan** to display the operating state of fan trays.

Examples

# Display the operating state of all fan trays.

```
<Sysname> display fan
Slot 1
      FAN    1
      State    : Normal
```

display job

Syntax

display job [*job-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

job-name: Specifies a job name, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display job** to display the jobs configured by using the **job** command.

If no job is specified, this command displays information about all scheduled jobs.

Related commands: **job**, **time**, and **view**.

Examples

# Display detailed information about the scheduled job **saveconfig**.

```
<Sysname> display job saveconfig
Job name: saveconfig
  Specified view: monitor
  Time 1: Execute command save 1.cfg after 40 minutes
```

The output shows that the current configuration will be automatically saved to the configuration file **1.cfg** in 40 minutes.

Table 21 Command output

Field	Description
Job name	Name of the scheduled job
Specified view	View for the commands to be executed
Time *timeID*	Execution time of each command in the job
Execute command	Command string

display memory

Syntax

display memory [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the memory usage statistics for an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

cpu *cpu-number*: Displays the memory usage statistics for a CPU. The *cpu-number* argument represents the ID of the CPU.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display memory** to display memory usage statistics.

If no IRF member switch is specified, the system displays the memory usage statistics for the master. If no CPU is specified, the system displays memory usage statistics for the main CPU.

Examples

# Display memory usage statistics.

```
<Sysname> display memory
System Total Memory(bytes): 70901280
Total Used Memory(bytes): 45706956
Used Rate: 64%
```

Table 22 Command output

Field	Description
System Total Memory(bytes)	Total size of the system memory (in bytes)
Total Used Memory(bytes)	Size of the memory used (in bytes)
Used Rate	Percentage of the memory used to the total memory

display power

Syntax

display power [**slot** *slot-number* [*power-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays information about the power supplies on an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

power-id: Displays information about a power supply. The *power-id* argument represents the power supply ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display power** to display power supply information.

Examples

# Display power supply information.

```
<Sysname> display power
Slot 1
      Power    1
      State     : Normal
      Type      : AC
```

Table 23 Command output

Field	Description
Slot 1	Power supply information of the device (whose member ID is 1)
Power	Power supply ID
State	Power supply state: • Normal • Absent • Fault
Type	Power supply type: • DC • AC

display reboot-type

Syntax

display reboot-type [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Displays the mode of the last reboot of an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display reboot-type** to display the mode of the last reboot.

If no IRF member switch is specified, the system displays the mode of the last reboot of the master.

Examples

# Display the mode of the last reboot of IRF member switch 1.

```
<Sysname> display reboot-type slot 1
  The rebooting type this time is: Cold
```

The output shows that the mode of the last reboot of member switch 1 is Cold boot (cold boot will restart a device by powering it on). (The display of Warm represents a warm boot, which means to restart a device by using the commands like **reboot**).

display rps

Syntax

display rps [**slot** *slot-number* [*rps-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the RPS status of an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch. If no member switch is specified, this command displays the RPS status for all IRF member switches.

rps-id: Displays the status of the specified RPS, where *rps-id* represents the RPS number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rps** to display RPS status information.

This command is available only for the devices that support RPS.

Examples

# Display RPS status information.

```
<Sysname> display rps
Slot 1
      Power    2
      State    : Absent
```

display schedule job

Syntax

display schedule job [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display schedule job** to display the job configured by using the **schedule job** command.

Related commands: **schedule job**.

Examples

# Display the job configured by using the **schedule job** command.

```
<Sysname> display schedule job
Specified command: execute 1.bat
Specified view: system view
Executed time: at 12:00 10/31/2010 (in 0 hours and 16 minutes)
```

If you change the system time within 16 minutes after you execute the **schedule job** command, the scheduled task becomes invalid. Then, if you execute the **display schedule job** command again, the system displays nothing.

Table 24 Command output

Field	Description
Specified command	Command to be executed
Specified view	View for the command to be executed
Executed time	Execution time of the command and the difference between the current system time and scheduled time

display schedule reboot

Syntax

display schedule reboot [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display schedule reboot** to display the reboot schedule.

Related commands: **schedule reboot at** and **schedule reboot delay**.

Examples

# Display the reboot schedule.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 03/10/2010 (in 2 hours and 5 minutes).
```

The output shows that the system will reboot at 16:00:00 on March 10, 2010 (in two hours and five minutes).

display system-failure

Syntax

display system-failure [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

3: Manage level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display system-failure** to display the exception handling method. In an IRF fabric, this command displays the exception handling method for all IRF member switches.

Related commands: **system-failure**.

Examples

# Display the exception handling method.

```
<Sysname> display system-failure
 System failure handling method: reboot
```

display transceiver

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the key parameters of the transceiver module in the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number. If no interface is specified, the command displays the key parameters of all transceiver modules.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display transceiver** to display key parameters of transceiver modules.

Examples

# Display the key parameters of the transceiver module in interface GigabitEthernet 1/0/3.

```
<Sysname> display transceiver interface gigabitethernet 1/0/3
GigabitEthernet1/0/3 transceiver information:
  Transceiver Type              : 1000_BASE_SX_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(m)          : 550(50um),270(62.5um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : HP
  Ordering Name                 : JD118B
```

Table 25 Command output

Field	Description
transceiver information	Transceiver module information
Transceiver Type	Transceiver module type
Connector Type	Connector type options: • SC—Fiber connector developed by NTT • LC—1.25 mm/RJ-45 fiber connector developed by Lucent • RJ-45 • CX 4
Wavelength(nm)	• Fiber transceiver: central wavelength (in nm) of the transmit laser. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma. • Copper transceiver: displayed as N/A.

Field	Description
Transfer distance(xx)	Transfer distance, with xx representing km for single-mode transceiver modules and m for other transceiver modules. If the transceiver module supports multiple transfer media, every two transfer distance values are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the supported transfer media: • 9 um—9/125 um single-mode fiber • 50 um—50/125 um multi-mode fiber • 62.5 um—62.5/125 um multi-mode fiber • TP—Twisted pair • CX4—CX4 cable
Digital Diagnostic Monitoring	Support for the digital diagnosis function: • YES—supported • NO—not supported
Vendor Name	Vendor name
Ordering Name	Product code

display transceiver alarm

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the alarms present on the transceiver module in the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number. If no interface is specified, the command displays present alarm information for all transceiver modules.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display transceiver alarm** to display alarms present on transceiver modules.

If no error occurs, **None** is displayed. Table 26 describes the transceiver module alarms that might occur.

Table 26 Common transceiver module alarms

Field	Remarks
SFP/SFP+	
RX loss of signal	Incoming (RX) signal is lost.
RX power high	Incoming (RX) power level is high.
RX power low	Incoming (RX) power level is low.
TX fault	Transmit (TX) fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XFP	
RX loss of signal	Incoming (RX) signal is lost.
RX not ready	RX is not ready
RX CDR loss of lock	RX clock cannot be recovered.
RX power high	RX power is high.
RX power low	RX power is low.
TX not ready	TX is not ready.
TX fault	TX fault
TX CDR loss of lock	TX clock cannot be recovered.
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Module not ready	Module is not ready.
APD supply fault	APD (Avalanche Photo Diode) supply fault
TEC fault	TEC (Thermoelectric Cooler) fault

Field	Remarks
Wavelength unlocked	Wavelength of optical signal exceeds the manufacturer's tolerance.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.

Examples

# Display the alarms present on the transceiver module in interface GigabitEthernet 1/0/3.

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/3
GigabitEthernet1/0/3 transceiver current alarm information:
  RX loss of signal
  RX power low
```

Table 27 Command output

Field	Description
transceiver current alarm information	Alarms present on the transceiver module.
RX loss of signal	Incoming (RX) signal is lost.
RX power low	Incoming (RX) power level is low.

display transceiver diagnosis

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the present measured values of the digital diagnosis parameters for the transceiver module in the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number. If no interface is specified, the command displays the present measured values of the digital diagnosis parameters for all transceiver modules.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display transceiver diagnosis** to display the present measured values of the digital diagnosis parameters for transceiver modules.

Examples

# Display the present measured values of the digital diagnosis parameters for the transceiver module in GigabitEthernet 1/0/3.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/3
GigabitEthernet1/0/3 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
```

Table 28 Command output

Field	Description
transceiver diagnostic information	Digital diagnosis parameters of the transceiver module in the interface.
Current diagnostic parameters	Current diagnostic parameters.
Temp.(°C)	Digital diagnosis parameter-temperature, in °C, with the precision to 1°C.
Voltage(V)	Digital diagnosis parameter-voltage, in V, with the precision to 0.01 V.
Bias(mA)	Digital diagnosis parameter-bias current, in mA, with the precision to 0.01 mA.
RX power(dBm)	Digital diagnosis parameter-RX power, in dBm, with the precision to 0.01 dBm.
TX power(dBm)	Digital diagnosis parameter-TX power, in dBm, with the precision to 0.01 dBm.

display transceiver manuinfo

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the electronic label data for the transceiver module in the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number. If no interface is specified, the command displays the electronic label data for all transceiver modules.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display transceiver manuinfo** to display the electronic label data for transceiver modules.

Examples

# Display the electronic label data for the transceiver module in GigabitEthernet 1/0/3.

```
<Sysname> display transceiver manuinfo interface gigabitethernet 1/0/3
GigabitEthernet1/0/3 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2011-03-01
  Vendor Name          : HP
```

Table 29 Command output

Field	Description
Manu. Serial Number	Serial number generated during debugging and testing of the customized transceivers.
Manufacturing Date	Debugging and testing date. The date takes the value of the system clock of the computer that performs debugging and testing.

display version

Syntax

display version [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display version** to display system version information, including the system software version.

Examples

# Display system version information.

```
<Sysname> display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 0000
Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
HP 5120-48G-PoE+ EI Switch with 2 Interface Slots uptime is 0 week, 0 day,
 0 hour, 53 minutes

HP 5120-48G-PoE+ EI Switch with 2 Interface Slots with 1 Processor
128M    bytes SDRAM
16384K  bytes Flash Memory

Hardware Version is REV.B
CPLD Version is 007
Bootrom Version is 607
[SubSlot 0] 48GE+4SFP+POE Hardware Version is REV.B
```

Table 30 Command output

Field	Description
HP Comware Platform Software	Software platform of the switch
Comware Software, Version 5.20, Release 0000	Software version, which comprises software platform name (Comware), platform version (Version 5.20), and product release version (Release 0000)
Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.	Copyright statement of the switch
HP 5120-48G-PoE+ EI Switch with 2 Interface Slots uptime is 0 week, 0 day, 0 hour, 53 minutes	Time duration for which the switch has been running since the last reboot
SDRAM	Memory size of the switch
Flash Memory	Flash size of the switch
Hardware Version is	Hardware version
CPLD Version	Version of the complex programmable logical device (CPLD)

Field	Description
Bootrom Version	Boot ROM version of the switch
[SubSlot 0]	Number of ports and hardware version

header

Syntax

header { **incoming** | **legal** | **login** | **motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

View

System view

Default level

2: System level

Parameters

incoming: Configures the banner displayed before a Modem dial-up user accesses user view. If authentication is required, the incoming banner appears after the authentication is passed.

legal: Configures the banner displayed before a user inputs the username and password to access the CLI.

login: Configures the banner displayed before password or scheme authentication is performed for a login user.

motd: Configures the greeting banner displayed before the legal banner appears.

shell: Configures the banner displayed before a non-modem dial-in user accesses user view.

text: Banner message, which can be input in two formats. For more information, see *Fundamentals Configuration Guide*.

Description

Use **header** to create a banner.

Use **undo header** to clear a banner.

Banners are greeting or alert messages that the system displays during the login process of a user.

Examples

# Configure banners.

```
<Sysname> system-view
[Sysname] header incoming %
Please input banner content, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Please input banner content, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Please input banner content, and quit with the character '%'.
Welcome to login(header login)%
```

```
[Sysname] header motd %
Please input banner content, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Please input banner content, and quit with the character '%'.
Welcome to shell(header shell)%
```

In this example, the percentage sign (%) is the starting and ending characters of text. Entering % after the displayed test quits the **header** command. As the starting and ending characters, % is not part of the banners.

# Verify the configuration by using Telnet. (The login authentication is not configured.)

```
******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Welcome to legal (header legal)
 Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to shell(header shell)
<Sysname>
```

# Verify the configuration by using Telnet. (Password authentication is configured.)

```
******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Welcome to legal (header legal)
 Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to login(header login)

Login authentication


Password:

Welcome to shell(header shell)
<Sysname>
```

job

Syntax

job *job-name*

undo job *job-name*

View

System view

Default level

3: Manage level

Parameters

job-name: Specifies the name of the scheduled job, a string of 1 to 32 characters.

Description

Use **job** to schedule a job or enter job view.

Use **undo job** to delete a scheduled job.

By default, no scheduled job is created.

You add commands to execute in a job in job view.

You can use the **job** command to schedule multiple jobs.

Related commands: **time** and **view**.

Examples

# Create a job **saveconfiguration** or enter its view.

```
<Sysname> system-view
[Sysname] job saveconfiguration
[Sysname-job-saveconfiguration]
```

reboot

Syntax

reboot [**slot** *slot-number*]

View

User view

Default level

3: Manage level

Parameters

slot *slot-number*: Specifies a switch. In an IRF fabric, if you do not specify this option, this command reboots all IRF member switches.

Description

Use **reboot** to reboot a switch or all IRF member switches.

You can use the **reboot** [**slot** *slot-number*] command on the master to reboot the master device or a subordinate device.

In an IRF fabric, if no member switch is specified, this command reboots all IRF member switches.

For data security, if you are performing file operations at the reboot time, the system does not reboot.

△ CAUTION:

- Device reboot can interrupt ongoing services.
- If the main system software image file has been corrupted or does not exist, the **reboot** command cannot reboot the switch. You must re-specify a main system software image file, or power off the switch and then power it on so the system can reboot with the backup system software image file.

Examples

# Reboot the device (The command output is omitted here).

```
<Sysname> reboot
```

reset unused porttag

Syntax

reset unused porttag

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset unused porttag** to clear unused 16-bit interface indexes.

A confirmation is required when you execute this command. The command will not run if you fail to make a confirmation within 30 seconds or enter **N** to cancel the operation.

Examples

# Clear unused 16-bit interface indexes.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]:y
<Sysname>
```

schedule job

Syntax

schedule job { **at** *time1* [*date*] | **delay** *time2* } **view** *view-name command*

undo schedule job

View

User view

Default level

3: Manage level

Parameters

at *time1* [*date*]: Specifies the execution time of a specified command.

- *time1*: Execution time of the command, in the *hh:mm* format. The *hh* value ranges from 0 to 23, and the *mm* value ranges from 0 to 59.
- *date*: Execution date of the command, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value ranges from 1 to 31.

delay *time2*: Specifies the execution waiting time of a specified command. *time2 represents the waiting time,* which can be in the following format:

- *hh*:*mm* format—The *hh* value ranges from 0 to 720, and the *mm* value ranges from 0 to 59. When the *hh* value is 720, the *mm* value cannot be more than 0.
- *mm* format—It ranges from 0 to 432000 minutes, with 0 indicating that the command is executed immediately.

view *view*: Specifies the view in which the command is executed. The *view* argument represents the view name, and it takes either of the following values at present:

- **shell**—Represents user view.
- **system**—Represents system view.

command: Command to be executed.

Description

Use **schedule job** to schedule a job.

Use **undo schedule job** to remove the job.

You can schedule a job to automatically run a command or a set of commands without administrative interference. The commands in a job are polled every minute. When the scheduled time for a command is reached, the job automatically executes the command. If a confirmation is required while the command is running, the system automatically enters **Y** or **Yes**. If characters are required, the system automatically enters a default character string or an empty character string when no default character string is available.

Follow these guidelines when you schedule a job in the non-modular approach:

- You can schedule only one job and run only one command in this approach. If you perform the **schedule job** command multiple times, the last configuration takes effect.
- To have the command successfully executed, check that the specified view and command are valid. The system does not verify their validity.
- If you specify both the *time1* and *date* arguments, the execution time or date must be later than the current system time or date.
- If you specify the *time1* argument, but not the *date* argument:
  - When *time1* is earlier than the current system time, the command runs at *time1* the next day.
  - When *time1* is later than the current system time, the command runs at *time1* of the current day.
- The interval between the scheduled time and the current system time cannot exceed 720 hours, or 30 days.
- Changing any clock setting can cancel the job set by using the **schedule job** command.
- After job execution, the configuration interface, view, and user status that you have before job execution restore even if the job has run a command that changes the user interface (for example,

telnet, **ftp**, and **ssh2**), the view (for example, **system-view** and **quit**), or the user status (for example, **super)**.

Examples

# Schedule a job to execute the batch file **1.bat** in system view in 60 minutes (assuming that the current time is 11:43).

```
<Sysname> schedule job delay 60 view system execute 1.bat
Info: Command execute 1.bat in system view will be executed at 12:43 10/31/2007 (in 1 hours
and 0 minutes).
```

# Schedule a job to execute the batch file **1.bat** in system view at 12:00 (assuming that the current time is 11:43).

```
<Sysname> schedule job at 12:00 view system execute 1.bat
Info: Command execute 1.bat in system view will be executed at 12:00 10/31/2007 (in 0 hours
and 16 minutes).
```

schedule reboot at

Syntax

schedule reboot at *hh:mm* [*date*]

undo schedule reboot

View

User view

Default level

3: Manage level

Parameters

hh:mm: Specifies a reboot time, in the *hh:mm* format. The *hh* value ranges from 0 to 23, and the *mm* value ranges from 0 to 59.

date: Specifies a reboot date, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value ranges from 1 to 31.

Description

Use **schedule reboot at** to schedule a reboot to occur at a specific time and date.

Use **undo schedule reboot** to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

The interval between the reboot date and the current date cannot exceed 30 x 24 hours, or 30 days.

When no reboot date is specified:

- If the reboot time is later than the current time, a reboot occurs at the reboot time of the current day.
- If the reboot time is earlier than the current time, a reboot occurs at the reboot time the next day.

The switch supports only one device reboot schedule. If you configure the **schedule reboot at** command multiple times, the last configuration takes effect. The **schedule reboot at** command and the **schedule reboot delay** command overwrite each other, and whichever is configured last takes effect.

The alert "REBOOT IN ONE MINUTE" appears one minute before the reboot time.

For data security, if you are performing file operations at the reboot time, the system does not reboot.

Related commands: **schedule reboot delay**.

△ CAUTION:

- Device reboot can interrupt network services.
- Changing any clock setting can cancel the reboot schedule.

Examples

# Configure the switch to reboot at 12:00 AM. This example assumes that the current time is 11:43.

```
<Sysname> schedule reboot at 12:00
Reboot system at 12:00 06/06/2010(in 0 hour(s) and 16 minute(s))
 confirm? [Y/N]:
```

Enter **y** at the prompt. If you have used the **terminal logging** command to enable the log display function (enabled by default) on the terminal, the system automatically displays a reboot schedule log message.

```
<Sysname>
%Jun  6 11:43:11:629 2010 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:43:11 06/06/2010, and system will
reboot at 12:00 06/06/2010.
```

schedule reboot delay

Syntax

schedule reboot delay { *hh:mm* | *mm* }

undo schedule reboot

View

User view

Default level

3: Manage level

Parameters

hh:mm: Specifies a time for the device reboot, in the *hh:mm* format. The *hh* value ranges from 0 to 720, and the *mm* value ranges from 0 to 59. When the *hh* value is 720, the *mm* value cannot be more than 0.

mm: Specifies a delay for the device reboot in minutes. The value ranges from 0 to 43,200.

Description

Use **schedule reboot delay** to schedule a reboot to occur after a delay.

Use **undo schedule reboot** to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

The reboot delay cannot exceed 30 x 24 x 60 minutes, or 30 days.

The switch supports only one device reboot schedule. If you configure the **schedule reboot delay** command multiple times, the last configuration takes effect. The **schedule reboot at** command and the **schedule reboot delay** command overwrite each other, and whichever is configured last takes effect.

The alert "REBOOT IN ONE MINUTE" appears one minute before the reboot time.

For data security, if you are performing file operations at the reboot time, the system does not reboot.

Related commands: **schedule reboot at**.

△ CAUTION:

- Device reboot can interrupt network services.
- Changing any clock setting can cancel the reboot schedule.

Examples

# Configure the switch to reboot in 88 minutes. This example assumes that the current time is 11:48.

```
<Sysname> schedule reboot delay 88
Reboot system at 13:16 06/06/2010(in 1 hour(s) and 28 minute(s)). confirm? [Y/N]:
```

Enter **y** at the prompt. If you have used the **terminal logging** command to enable the log display function (enabled by default) on the terminal, the system automatically displays a reboot schedule log message.

```
<Sysname>
%Jun  6 11:48:44:860 2010 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:48:44 06/06/2010, and system will
reboot at 13:16 06/06/2010.
```

shutdown-interval

Syntax

shutdown-interval *time*

undo shutdown-interval

View

System view

Default level

2: System level

Parameters

time: Specifies the port status detection timer in seconds, which ranges from 0 to 300.

Description

Use **shutdown-interval** to set the port status detection timer.

Use **undo shutdown-interval** to restore the default.

By default, the timer is 30 seconds.

Some protocols might shut down ports under specific circumstances. For example, MSTP shuts down a BPDU guard enabled port when the port receives a BPDU. Then, the device starts the detection timer. If the port is still down when the detection timer expires, the port quits the shutdown status and resume its actual physical status.

- If you change the detection timer to T1 during port detection, the timer from when you change the timer to the time when the protocol module shuts down the port is T. If T<T1, the port resume its actual physical status after T1-T time. If T>=T1, the port resume its actual physical status immediately. For example, if the detection timer is set to 30 seconds and you change it to 10 seconds (T1=10) two seconds after the port is shut down (T=2), this port resume its actual physical status 8 seconds later. If the detection timer is set to 30 seconds and you change it to 2 seconds ten seconds after the port is shut down, this port resume its actual physical status immediately.

- If the detection timer is set to 0, the protocol module will never automatically recover the port. You need to manually bring up the port by using the **undo shutdown** command or change the detection timer to a non-zero value.

Examples

# Set the port status detection timer to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

startup bootrom-access enable

Syntax

startup bootrom-access enable

undo startup bootrom-access enable

View

User view

Default level

2: System level

Parameters

None

Description

Use **startup bootrom-access enable** to enable Boot ROM access during system startup (that is, you can press **Ctrl+B** to enter the Boot ROM menu).

Use **undo startup bootrom-access enable** to disable Boot ROM access during system startup (that is, you cannot enter the Boot ROM menu no matter whether you press **Ctrl+B** or not).

By default, Boot ROM access during system startup is enabled.

Related commands: **display startup**.

Examples

# Disable Boot ROM access during system startup.

```
<Sysname> undo startup bootrom-access enable
```

sysname

Syntax

sysname *sysname*

undo sysname

View

System view

Default level

2: System level

Parameters

sysname: Name of the device, which is a string of 1 to 30 characters.

Description

Use **sysname** to set the device name.

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

The default device name is **HP**.

A device name identifies a device in a network and works as the user view prompt at the CLI. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

Examples

# Set the name of the device to **S2000**.

```
<Sysname> system-view
[Sysname] sysname S2000
[S2000]
```

system-failure

Syntax

system-failure { **maintain** | **reboot** }

undo system-failure

View

System view

Default level

3: Manage level

Parameters

maintain: Specifies that when the system detects any software abnormality, it maintains the current situation, and does not take any measure to recover itself.

reboot: Specifies that when the system detects any software abnormality, it recovers itself through automatic reboot.

Description

Use **system-failure** to configure the exception handling method on all IRF member switches.

By default, all IRF member switches adopt the **reboot** method to handle exceptions.

The exception handling method is effective to only the failed member switch, and does not influence the operations of other IRF member switches.

Examples

# Set the exception handling method to **reboot**.

```
<Sysname> system-view
[Sysname] system-failure reboot
```

temperature-limit

Syntax

temperature-limit slot *slot-number* **hotspot** *sensor-number lowerlimit warninglimit*

undo temperature-limit slot *slot-number* **hotspot** *sensor-number*

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch. The *slot-number* argument represents the IRF member ID of the switch.

hotspot: Specifies a hotspot sensor, which is typically placed near the chip that generates a great amount of heat and is used for temperature monitoring.

sensor-number: Specifies a sensor by its number. The sensor number is always 1.

lowerlimit: Specifies a lower threshold in Celsius degrees. The value ranges from –10°C to +70°C (14°F to 158°F).

warninglimit: Specifies a warning threshold in Celsius degrees. The value ranges from 20°C to 120°C (68°F to 248°F).

Description

Use **temperature-limit** to set the temperature thresholds for the device.

Use **undo temperature-limit** to restore the default.

By default, the lower threshold is –5°C (23°F), and the warning threshold is 55°C (131°F).

When the device temperature drops below the lower threshold or reaches the warning threshold, the device logs the event and outputs a log message and a trap.

The warning threshold must be higher than the lower threshold.

Related commands: **display environment**.

Examples

# Set the lower threshold for the hotspot sensor 1 on the IRF member switch 1 to 0°C (32°F), and the warning threshold to 100°C (212°F).

```
<Sysname> system-view
[sysname] temperature-limit slot 1 hotspot 1 0 100
```

time at

Syntax

time *time-id* **at** *time date* **command** *command*

time *time-id* { **one-off** | **repeating** } **at** *time* [**month-date** *month-day* | **week-day** *week-daylist*] **command** *command*

undo time *time-id*

View

Job view

Default level

3: Manage level

Parameters

time *timeid*: Time setting entry, an integer that ranges from 1 to 10.

at *time*: Specifies an execution time, in the *hh:mm* format, where the *hh* value ranges from 0 to 23 and the *mm* value ranges from 0 to 59.

one-off: Specifies that the specified command is executed for once.

repeating: Specifies a recurring time schedule.

date: Specifies the execution date, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value ranges from 1 to 31. The specified execution date must be ahead of the current date.

month-date *month-day*: Specifies the date for executing the command. The *month-day* argument specifies the date, and ranges from 1 to 31.

week-day *week-daylist*: Specifies the day or days for executing the command. The *week-daylist* argument specifies one day or up to seven days, which can be any combination of Sun, Mon, Tue, Wed, Thu, Fri, and Sat. For example, to have a command executed on Monday, you can enter **week-day** Mon; to have a command executed on Friday and Saturday, enter **week-day** Fri Sat. Use a space between every two days for separation.

command *command*: Specifies the command to be automatically executed, in the text format. The command must be executable in the view specified by the **view** command. Otherwise this command cannot be automatically executed. Therefore, ensure the correctness of the configuration.

Description

Use **time at** to add a command in the job schedule.

Use **undo time** to remove a command from the job schedule.

The commands in a job must be in the same view.

Every job can have up to 10 commands.

Changing a clock setting does not affect the schedule set by using the **time at** command.

The time ID (*time-id*) must be unique in a job. If two time and command bindings have the same time ID, the one configured last takes effect.

Use Table 31 when you add commands in a job.

Table 31 Command schedule options

Command	Description
time timeid **at** time date **command** *command*	Schedules a command to run at a specific time and date. The time or date must be later than the current system time or date.
time *timeid* **one-off at** *time* **command** *command*	Schedules a command to run at a specific time on the current day. If the specified time has passed, the command runs the next day. The command runs only once.

Command	Description
time *timeid* **one-off at** *time* **month-date** *month-day* **command** *command*	Schedules a command to run at a specific day in the current month. If the specified time or day has passed, the command runs in the next month. The command runs only once.
time *timeid* **one-off at** *time* **week-day** *week-daylist* **command** *command*	Schedules a command to run at a specific time on a specific day or days in the current week. If the specified time or day has passed, the command runs in the next week. The command runs only once.
time *timeid* **repeating at** *time* **command** *command*	Schedules a command to run at a specific time every day.
time *timeid* **repeating at** *time* **month-date** *month-day* **command** *command*	Schedules a command to run on a specific day every month.
time *timeid* **repeating at** *time* **week-day** *week-daylist* **command** *command*	Schedules a command to run at a specific time in a specific day or days every week.

Related commands: **job** and **view**.

Examples

# Schedule a job to save the configuration file **a.cfg** at 3:00 on May 18, 2011.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 at 3:00 2011/05/18 command save a.cfg
```

# Schedule a job to save the configuration file at 12:00 every day.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 repeating at 12:00 command save a.cfg
```

# Schedule a job to save the configuration file at 8:00 AM on 5th in the current month, which might be executed in the second month if the time has passed.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 one-off at 8:00 month-date 5 command save a.cfg
```

# Schedule a job to save the configuration file at 8:00 AM on 5th every month.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 repeating at 8:00 month-date 5 command save a.cfg
```

# Schedule a job to save the configuration file at 8:00 AM on Friday and Saturday in the current week, which might be delayed to the next week if the time has passed.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 one-off at 8:00 week-day fri sat command save a.cfg
```

# Schedule a job to save the configuration file at 8:00 every Fridays and Saturdays.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 repeating at 8:00 week-day fri sat command save a.cfg
```

time delay

Syntax

time *time-id* { **one-off** | **repeating** } **delay** *time* **command** *command*

undo time *time-id*

View

Job view

Default level

3: Manage level

Parameters

time *timeid*: Time setting entry, an integer that ranges from 1 to 10.

one-off: Specifies that the specified command is executed for once.

repeating: Specifies a recurring time schedule.

delay *time*: Specifies the delay time for executing the command, in the *hh:mm* format or *mm* format.

- When the time argument is in the *hh:mm* format, the *hh* value ranges from 0 to 720, and the *mm* value ranges from 0 to 59. When the *hh* value is 720, the *mm* value can be only 00.
- When the time argument is in the *mm* format, the *mm* value ranges from 1 to 43200. That is, the maximum value of the delay timer is 30 days.

command *command*: Specifies the command to be automatically executed, in the text format. The specified command must be a complete command without interactive input.

Description

Use **time delay** to add a command to run after a delay in the job schedule.

Use **undo time** to remove the configuration.

The commands in a scheduled job must be in the same view.

Every job can have up to 10 commands.

Changing a clock setting does not affect the schedule set by using the **time delay** command.

The time ID (*time-id*) must be unique in a job. If two time and command bindings have the same time ID, the one configured last takes effect.

Use Table 32 when you add commands in a job.

Table 32 Command schedule options

Command	Description
time *timeid* **one-off delay** *time2* **command** *command*	Schedules a command to run after a delay time. The command runs only once.

Command	Description
time *timeid* **repeating delay** *time2* **command** *command*	Schedules a command to run every the delay time.

Related commands: **job** and **view**.

Examples

# Save the configuration file five minutes later.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 one-off delay 5 command save a.cfg
```

# Save the configuration file every five minutes.

```
<Sysname> system-view
[Sysname] job saveconfig
[Sysname-job-saveconfig] view monitor
[Sysname-job-saveconfig] time 1 repeating delay 5 command save a.cfg
```

view

Syntax

view *view-name*

undo view

View

Job view

Default level

3: Manage level

Parameters

view-name: Specifies a view in which commands in the job run. A view name is a string of 1 to 90 characters.

Description

Use **view** to specify the view in which the commands in the job run.

Use **undo view** to remove the configuration.

By default, no view is specified for the scheduled job.

Every job can have only one view. If you specify multiple views, the one specified the last takes effect.

Input a view name in its complete form. Most commonly used view names include **monitor** for user view, **system** for system view,**GigabitEthernetx/x/x** for Ethernet interface view, and **Vlan-interfacex** for VLAN interface view.

Related commands: **job** and **time**.

Examples

# Specify the view in which the commands in the job run.

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

```
[Sysname] job creatvlan
[Sysname-job-creatvlan] view system
```

Index

Contents

IRF configuration commands

display irf

Syntax

display irf [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display irf** to display IRF fabric information, including the member ID, role, priority, bridge MAC address, and description of each IRF member.

Examples

# Display IRF fabric information.

```
<Sysname> display irf
Switch  Role     Priority    CPU-Mac           Description
   1     Slave    1            000f-e2be-3102   F1Num001
 *+2     Master  1            00e0-fcb1-ade2   F1Num002
--------------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 00e0-fc00-1000
 Auto upgrade                  : yes
 Mac persistent                : always
 Domain ID                      : 30
```

Table 1 Command output

Field	Description
Switch	IRF member ID: - ID of the master is prefixed with an asterisk (*) sign. - ID of the device where you have been logged in is prefixed with a plus (+) sign.
Role	Switch role in the IRF fabric: - **Slave**—The switch is a subordinate device. - **Master**—The switch is the master. - **SlaveWait**—The switch is joining the IRF fabric as a subordinate device. - **Loading**—The switch is loading the system software image.
CPU-MAC	CPU MAC address of the switch.
Description	Description you have configured for the member device. - If no description is configured, this field displays a dashed line (-----). - If the description exceeds the maximum number of characters that can be displayed, an ellipsis (…) is displayed in place of the exceeding text. To display the complete description, use the **display current-configuration** command.
Auto upgrade	Status of the software auto-update function: - **yes**—Enabled. The master switch automatically propagates its system software image to the switch you are adding to the IRF fabric. - **no**—Disabled. You must manually make sure the joining switch uses the same system software image as the master switch. If not, the new switch cannot join the IRF fabric.
MAC persistent	IRF bridge MAC persistence setting: - **6 min**—Bridge MAC address of the IRF fabric persists for six minutes after the master leaves. - **always**—Bridge MAC address of the IRF fabric does not change after the master leaves. - **no**—Bridge MAC address of the new master replaces the original one as soon as the old master leaves.
Domain ID	Domain ID assigned to the IRF fabric. A domain ID uniquely identifies an IRF fabric on a network that has multiple IRF fabrics.

display irf configuration

Syntax

display irf configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display irf configuration** to display the basic IRF settings.

The command displays each member's current member ID, new member ID, priority, IRF port state, and IRF port bindings.

The new member ID take effect after the switch reboots.

Examples

# Display the basic IRF settings.

```
<Sysname> display irf configuration
MemberID NewID    IRF-Port1                     IRF-Port2
  1        1        GigabitEthernet1/1/1         disable
  2        2        disable                         Ten-GigabitEthernet2/2/1
```

Table 2 Command output

Field	Description
MemberID	Current member ID.
NewID	Member ID that will take effect after a reboot.
IRF-Port1	Physical port or ports bound to IRF port 1. If no physical ports are bound to the IRF port, this field displays **disable**.
IRF-Port2	Physical port or ports bound to IRF port 2. If no physical ports are bound to the IRF port, this field displays **disable**.

display irf topology

Syntax

display irf topology [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display irf topology** to display the IRF fabric topology.

Command output includes member IDs, IRF port state, and adjacencies of IRF ports.

Examples

# Display the IRF fabric topology.

```
<Sysname> display irf topology
                          Topology Info
 -------------------------------------------------------------------------
               IRF-Port1                IRF-Port2
 Switch    Link       neighbor      Link       neighbor    Belong To
 2         DOWN        --             UP           1           0023-8927-ad54
 1         UP          2              DIS          --          0023-8927-ad54
```

Table 3 Command output

Field	Description
Switch	Member ID.
IRF-Port 1	Link state and neighbor switch of IRF port 1.
IRF-Port 2	Link state and neighbor switch of IRF port 2.
Link	Link state of the IRF port: - **UP**—IRF link is up. - **DOWN**—IRF link is down. - **DIS**—No physical ports have been bound to the IRF port. You must use the **port group interface** command to bind at least one physical port to the IRF port.
neighbor	IRF member ID of the switch connected to the IRF port. If no device is connected to the IRF port, this field displays two hyphens (--).
Belong To	IRF fabric that has the switch, represented by the CPU MAC address of the master in the IRF fabric.

display irf-port load-sharing mode

Syntax

display irf-port load-sharing mode [**irf-port** [*member-id/port-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

irf-port: Displays IRF port specific load sharing modes.

member-id/port-number: Specifies an IRF port number. The *member-id* argument represents an IRF member ID. The *port-number* argument represents the index number (1 or 2) of the IRF port on the member device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display irf-port load-sharing mode** to display IRF link load sharing mode.

To display the global load sharing mode for IRF links, execute this command without any keyword or argument.

To display the load sharing mode used on each IRF port in the IRF fabric, specify the **irf-port** keyword but not any IRF port.

To display the load sharing mode used on a specific IRF port, specify both the **irf-port** keyword and the *member-id/port-number* argument.

Examples

# Display the global IRF link load sharing mode. In this example, because no user-defined global load sharing mode has been configured, the default global load sharing mode applies.

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

# Display the global IRF link load sharing mode. In this example, because a global sharing mode based on source and destination IP addresses have been configured, the configured mode applies.

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
  destination-ip address,  source-ip address
```

# Display the load sharing mode of IRF port 1/1. In this example, because neither port-specific load sharing mode nor user-defined global load sharing mode has been configured, the default global load sharing mode applies.

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port1/1 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

# Display the load sharing mode used on IRF port 1/1.

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port1/1 Load-Sharing Mode:
  destination-mac address, source-mac address
```

# Display the load sharing mode used on each IRF port.

```
<Sysname> display irf-port load-sharing mode irf-port
irf-port 1/1 Load-Sharing Mode:
  destination-mac address, source-mac address
irf-port 1/2 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Table 4 Command output

Field	Description
irf-port Load-Sharing Mode	Global load sharing mode for IRF links: • If no user-defined global load sharing mode has been configured, the default global load sharing mode applies. • If a user-defined global load sharing mode has been configured, the configured mode applies.
irf-port 1/1 Load-Sharing Mode	Load sharing mode for IRF-port 1/1: • If you have not configured a port-specific load sharing mode, the global IRF link load sharing mode applies. • If you have configured a port-specific load sharing mode, the configured mode applies.
Layer 2 traffic: destination-mac address, source-mac address	Default load sharing mode for traffic that has no IP header. By default, this type of traffic is distributed based on source and destination MAC addresses.
Layer 3 traffic: destination-ip address, source-ip address	Default load sharing mode for IP packets. By default, this type of traffic is distributed based on source and destination IP addresses.
destination-mac address, source-mac address	User-configured IRF link load sharing criteria. In this sample output, the criteria are source and destination MAC addresses. Information displayed in this field depends on user configuration.

display mad

Syntax

display mad [**verbose**] [**\|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about the MAD detection. If this keyword is not provided, the system displays brief information about the MAD detection.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mad** to display MAD status and settings.

Examples

# Display brief MAD information.

```
<Sysname> display mad
MAD ARP disabled.
MAD LACP disabled.
```

# Display detailed MAD information.

```
<Sysname> display mad verbose
Current MAD status: Detect
Excluded ports(configurable):
  Vlan-interface999
Excluded ports(can not be configured):
  Ten-GigabitEthernet1/1/1
MAD ARP enabled interface:
  Vlan-interface2
MAD enabled aggregation port:
  Bridge-Aggregation1
```

Table 5 Command output

Field	Description
Current MAD status	MAD status: • **Detect**—The IRF fabric is integrated. • **Recovery**—IRF fabric is in Recovery state. When detecting a multi-active collision, MAD places the IRF fabric with higher master ID in Recovery state and shuts down all physical ports in the fabric but IRF physical ports and ports that are configured to not shut down. • **Detect to Recovery**—State of the IRF fabric is transitioning from Detect to Recovery, for example, as the result of an IRF split. • **Recovery to Detect**—State of the IRF fabric is transitioning from Recovery to Detect.
Excluded ports(configurable)	Ports manually configured to not shut down when the IRF fabric transitions to the Recovery state.
Excluded ports(can not be configured)	Ports automatically set by the system to not shut down when the IRF fabric transitions to the Recovery state.
MAD ARP enabled interface: Vlan-interface2	Interface where ARP MAD is enabled.
MAD enabled aggregation port: Bridge-Aggregation1	Aggregate interface where LACP MAD is enabled.

display switchover state

Syntax

display switchover state [**slot** *member-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *member-id*: Specifies an IRF member by its member ID. If no IRF member is specified, this command displays the master/subordinate switchover states of the master.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display switchover state** to display the master/subordinate switchover states of IRF member switches.

Examples

# Display the master/subordinate switchover states of the master.

```
<Sysname> display switchover state
Master HA State to slot 2: Slave is absent.
Master HA State to slot 3: Realtime backup to slave.
Master HA State to slot 4: Waiting batch backup request from slave.
```

Table 6 Command output for the master

Field	Description
Master HA State to slot *slot-number*	Describes the master/subordinate switchover state between the master and a specific member. The *slot-number* argument represents an IRF member ID.
Slave is absent	The IRF member ID is not used in this IRF fabric.
Waiting batch backup request from slave	The master switch is waiting for the batch backup request from the subordinate switch.
Batch backup	The subordinate switch is bulk-backing up data from the master.
Realtime backup to slave	The subordinate switch is backing up real-time data from the master switch.
Data smooth	The subordinate switch is transitioning to be the master.

# Display the master/subordinate switchover state of member switch 3.

```
<Sysname> display switchover state slot 3
Slave HA State: Receiving realtime data.
```

Table 7 Command output for a subordinate

Field	Description
Slave HA State	Describes the master/subordinate switchover state of the subordinate switch.
Waiting	The subordinate switch is ready for bulk-backing up data.
Sending batch backup request	The subordinate switch is requesting for a bulk-backup.
Receiving batch data	The subordinate switch is bulk backing up data.
Receiving realtime data	The member switch is receiving real-time data.

irf auto-update enable

Syntax

irf auto-update enable

undo irf auto-update enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **irf auto-update enable** to enable the software auto-update function for propagating the system software image of the master to all its members.

Use **undo irf auto-update enable** to disable this function.

By default, software auto-update for subordinate switches is enabled.

When you add a switch to the IRF fabric, the software auto-update function compares the system software versions of the switch and the IRF master. If the versions are different, the switch automatically downloads the system software image from the master, sets the downloaded file as the system software for the next reboot, and automatically reboots with the new system software image to re-join the IRF fabric.

To avoid an update failure, make sure the switch has efficient space for the new system software image.

If the switch you are adding to the IRF fabric is incompatible with the software version running on the master, the software auto-update function cannot work correctly.

If software auto-update function is disabled, you must manually update the switch with the system software image of the master.

Examples

# Enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
```

irf domain

Syntax

irf domain *domain-id*

undo irf domain

View

System view

Default level

3: Manage level

Parameters

domain-id: Specifies a domain ID for the IRF fabric. The value range is 0 to 4294967295.

Description

Use **irf domain** to assign a domain ID to an IRF fabric.

Use **undo irf domain** to restore the default IRF domain ID.

The default domain IRF domain ID is 0.

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

If you use a member in one IRF fabric as the intermediate device for performing ARP MAD or LACP MAD for another IRF fabric, assign the two IRF fabrics different domain IDs to avoid false detection of IRF split.

Examples

# Set the IRF domain ID to 30.

```
<Sysname> system-view
[Sysname] irf domain 30
```

irf link-delay

Syntax

irf link-delay *interval*

undo irf link-delay

View

System view

Default level

3: Manage level

Parameters

interval: Sets the IRF link down report delay in milliseconds. The value range is 0 to 30000.

Description

Use **irf link-delay** to set the delay for the IRF ports in the IRF fabric to report a link down event.

Use **undo irf link-delay** to restore the default.

By default, the IRF link down event report delay is 4 seconds.

An IRF link down report delay helps avoid link flapping causing frequent IRF splits and merges during a short time.

An IRF port handles link down and link up events, as follows:

- If the IRF link changes from up to down, the port does not immediately report the change to the IRF fabric. If the IRF link state is still down when the delay time is reached, the port reports the change to the IRF fabric.
- If the IRF link changes from down to up, the link layer immediately reports the event to the IRF fabric.

Examples

# Set the IRF link down report delay to 300 milliseconds.

```
<Sysname> system-view
[Sysname] irf link-delay 300
```

irf mac-address persistent

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

View

System view

Default level

3: Manage level

Parameters

always: Enables the IRF bridge MAC address to persist forever regardless of master re-election or leaving of the master.

timer: Enables the IRF bridge MAC address to remain the same for six minutes after the master device leaves. If the device re-joins the IRF fabric before the time limit is reached, the IRF bridge MAC address does not change. If not, the IRF fabric uses the bridge MAC address of the new master as the IRF bridge MAC address.

Description

Use **irf mac-address persistent** to configure IRF bridge MAC persistence so the IRF fabric continues using the bridge MAC address of the old master as its bridge MAC address for a period of time after a master re-election.

Use **undo irf mac-address persistent** to disable IRF bridge MAC persistence so the IRF fabric changes its bridge MAC address as soon as the master leaves.

By default, after the master device leaves, the IRF fabric continues using its bridge MAC address as the IRF bridge MAC address for six minutes.

An IRF fabric by default uses the bridge MAC address of the master device as its bridge MAC address. This bridge MAC address is used by Layer 2 protocols, for example, LACP, to identify the IRF fabric, and must be unique on a switched LAN for proper communication.

To avoid duplicate bridge MAC addresses, an IRF fabric can automatically change its bridge MAC address after its master leaves, but the change causes temporary service interruption. To avoid this situation, configure bridge MAC persistence.

If two IRF fabrics have the same bridge MAC address, they cannot be merged into one IRF fabric.

If ARP MAD is used, you must use the **undo irf mac-address persistent** command disable IRF bridge MAC persistence.

Examples

# Enable the IRF bridge MAC address to persist forever.

```
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

irf member description

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

View

System view

Default level

3: Manage level

Parameters

member-id: Specifies the ID of an IRF member.

text: Configures the IRF member description, a string of 1 to 127 characters.

Description

Use **irf member description** to configure a description for an IRF member.

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

By default, no description is configured for any IRF member.

Examples

# Configure a description for IRF member 1.

```
<Sysname> system-view
[Sysname] irf member 1 description F1Num001
```

irf member priority

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

View

System view

Default level

3: Manage level

Parameters

member-id: Specifies an IRF member ID.

priority: Sets priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

Description

Use **irf member priority** to change the priority of an IRF member.

Use **undo irf member priority** to restore the default.

By default, the priority of a member switch is 1.

Examples

Change the member priority assignment scheme in the IRF fabric so member 2 takes over as the master at the next master election:

# Display IRF fabric information.

```
<Sysname> display irf
 Switch    Role    Priority    CPU-Mac
  +1       Slave    29           00e0-fc00-1115
   2       Slave    1            00e0-fc00-1615
  *3       Master   32          00e0-fc00-1015
   9       Slave    30          00e0-fc00-1515
--------------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
 The Bridge MAC of the IRF is: 00e0-fc00-1000
 Auto upgrade                  : yes
 Mac persistent                : always
```

# Change the priority of the current master (member ID 3) to 16.

```
<Sysname> system-view
[Sysname] irf member 3 priority 16
```

# Change the priority of member 2 to 32.

```
<Sysname> system-view
[Sysname] irf member 2 priority 32
```

irf member renumber

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

View

System view

Default level

3: Manage level

Parameters

member-id: Specifies the current ID of an IRF member switch. The value range is 1 to 4.

new-member-id: Assigns a new ID to the IRF member switch. The value range is 1 to 4.

Description

Use **irf member renumber** to change the IRF member ID of a switch.

Use **undo irf member renumber** to set the IRF member ID of a switch to 1.

By default, the IRF member ID is 1.

> △ CAUTION:
>
> In an IRF fabric, changing IRF member IDs might cause undesirable configuration changes and even data loss. Before you do that, back up the configuration and make sure you fully understand the impact on your network. For example, all member switches in an IRF fabric are the same model. If you swapped the IDs of any two members, their interface settings would also be swapped.

To create an IRF fabric, you must assign a unique IRF member ID to each switch.

Assigning IRF member IDs before the IRF fabric is formed. To prevent any undesirable configuration change or data loss, avoid changing member IDs after the IRF fabric is formed.

The new member ID takes effect at a reboot. After the switch reboots, the settings on all member-ID related physical resources (including common physical network ports) are removed and require reconfiguration, regardless of whether you have saved the configuration.

To cancel the change before you reboot the member switch, use the **irf member renumber** command rather its **undo** form. In the command, set the new member ID to be the same as the old member ID.

Examples

# Change the member ID of an IRF member from 1 to 3.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Warning: Renumbering the switch number may result in configuration change or loss.
Continue?[Y/N]:Y
```

# Change the member ID of an IRF member from 2 to 4.

```
<Sysname> system-view
[Sysname] irf member 2 renumber 4
Warning: Renumbering the switch number may result in configuration change or loss.
Continue?[Y/N]y
```

# Cancel the change in the preceding example before rebooting the switch.

```
[Sysname] undo irf member 2 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss.
Continue?[Y/N]y
```

irf switch-to

Syntax

irf switch-to *member-id*

View

System view

Default level

3: Manage level

Parameters

member-id: Specifies the member ID of a subordinate member. The *member-id* argument cannot take the member ID of the master switch.

Description

Use **irf switch-to** to access a subordinate switch's CLI from the master's CLI.

When you log in to an IRF fabric, you are placed at the CLI of the master, regardless of at which member switch you are logged in. After that, you can access the CLI of a subordinate switch to execute a limited set of maintenance commands.

At the CLI of a subordinate switch, you are placed in user view, and the command prompt changes to *<Sysname-Slave#member-ID/slot-number>*, for example, <Sysname-Slave#2>. You can use the following commands at a subordinate switch's CLI:

- **display**
- **quit**
- **return**
- **system-view**
- **debugging**
- **terminal debugging**
- **terminal trapping**
- **terminal logging**

To return to the CLI of the master switch, use the **quit** command.

Examples

# Log in to the CLI of IRF member switch 2.

```
<Sysname> system-view
[Sysname] irf switch-to 2
<Sysname-Slave#2>
```

irf-port

Syntax

irf-port *member-id/port-number*

undo irf-port *member-id/port-number*

View

System view

Default level

3: Manage level

Parameters

member-id/port-number: Specifies an IRF port number. The *member-id* argument represents the IRF member ID. The *port-number* argument represents the index of the port on the member switch, and must be 1 or 2.

Description

Use **irf-port** to create an IRF port or enter IRF port view.

Use **undo irf-port** to delete an IRF port.

By default, no IRF port is created.

To set up an IRF link between two switches, you must enter IRF port view to bind physical ports to the IRF port used by each switch for IRF connection.

Related commands: **port group interface**.

Examples

# Create IRF port 1 on IRF member 3 and bind Ten-GigabitEthernet 3/1/1 to the IRF port.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/1/1
[Sysname-Ten-GigabitEthernet3/1/1] shutdown
[Sysname-Ten-GigabitEthernet3/1/1] quit
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/1/1
[Sysname-irf-port3/1] quit
[Sysname] interface ten-gigabitethernet 3/1/1
[Sysname-Ten-GigabitEthernet3/1/1] undo shutdown
```

irf-port load-sharing mode

Syntax

irf-port load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo irf-port load-sharing mode

View

System view, IRF port view

Default level

3: Manage level

Parameters

destination-ip: Distributes traffic across IRF member links based on destination IP address.

destination-mac: Distributes packets across IRF member links based on destination MAC address.

source-ip: Distributes packets across IRF member links based on source IP address.

source-mac: Distributes packets across IRF member links based on source MAC address.

Description

Use **irf-port load-sharing mode** to set the global or port-specific load sharing mode for IRF links.

Use **undo irf-port load-sharing mode** to restore the default.

By default, traffic that has no IP header is distributed by source and destination MAC addresses, and IP traffic is distributed by source and destination IP addresses.

On an IRF port that has multiple links, traffic is balanced across its physical links. You can configure the IRF port to distribute traffic based on source IP address, destination IP address, source MAC address, destination address, or a combination of them. If a criteria combination is not supported, the system displays an error message.

Configure the global IRF link load sharing mode in system view, and configure a port-specific load sharing mode in IRF port view. To successfully configure a load sharing mode for an IRF port, make sure you have bound at least one physical port to the IRF port.

An IRF port preferentially uses the port-specific load sharing mode. If no port-specific load sharing mode is available, it uses the global load sharing mode. If no global load sharing mode is configured, the default load sharing mode applies.

Examples

# Configure the global IRF link load sharing mode to distribute traffic based on destination MAC address.

```
<Sysname> system-view
[Sysname] irf-port load-sharing mode destination-mac
```

# Configure IRF port 1/1 to distribute traffic across its physical links based on destination MAC address.

```
<Sysname> system-view
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] irf-port load-sharing mode destination-mac
```

irf-port-configuration active

Syntax

irf-port-configuration active

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **irf-port-configuration active** to activate IRF ports.

After connecting the physical ports between two switches and bind them to the correct IRF ports, you must activate the settings on the IRF ports to merge the two switches into one IRF fabric. After an IRF port is activated, its link state in the **display irf topology** command output changes from **DIS** or **DOWN** to **UP**.

You do not need to activate the IRF port settings if the configuration file that the switch starts with has included IRF port bindings or you are binding more physical ports to an IRF port after an IRF fabric is formed. The system automatically does the work.

Activating IRF port settings can cause IRF merge and device reboot. To avoid configuration loss, follow this procedure to set up your IRF fabric:

1. Plan the IRF setup, including the IRF fabric topology, IRF fabric size, member ID assignment, and bindings of physical ports and IRF ports.
2. Change the IRF member ID of each switch to make sure they are unique in the IRF fabric.
3. Connect the physical ports between neighboring switches and make sure that the peer ports can reach each other.
4. Create IRF ports on each switch.
5. Bind the physical ports to the IRF ports on each switch.

6. Save the configuration to the next-startup configuration file on each switch.
7. Activate the IRF ports on each switch.

Examples

To configure and activate IRF port 1/2:

# Create IRF port 1/2 and bind Ten-GigabitEthernet1/1/2 to it.

```
<Sysname> system-view
[Sysname] interface ten-gigabitEthernet 1/1/2
[Sysname-Ten-GigabitEthernet1/1/2] shutdown
[Sysname-Ten-GigabitEthernet1/1/2] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface Ten-GigabitEthernet 1/1/2
[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitEthernet 1/1/2
[Sysname-Ten-GigabitEthernet1/1/2] undo shutdown
[Sysname-Ten-GigabitEthernet1/1/2] quit
```

# Save the configuration so the IRF port settings can take effect after the switch reboots.

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/aa.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait............................
 Saved the current configuration to mainboard device successfully.
Slot 1:
 Save next configuration file successfully.
 Configuration is saved to device successfully.
```

# Activate the IRF port.

```
[Sysname] irf-port-configuration active
```

mad arp enable

Syntax

mad arp enable

undo mad arp enable

View

VLAN interface view

Default level

3: Manage level

Parameters

None

Description

Use **mad arp enable** to enable ARP MAD.

Use **undo mad arp enable** to disable ARP MAD.

By default, ARP MAD is disabled.

You can set up ARP MAD links between neighbor IRF members or more commonly, between each IRF member device and an intermediate device.

When you configure ARP MAD, follow these guidelines:

- If an intermediate device is used, you can use common data links as ARP MAD links. If no intermediate device is used, set up dedicated ARP MAD links between IRF member devices.
- Use a VLAN dedicated to ARP MAD.
- If an intermediate device is used, do the following:
  - Run the spanning tree feature between the IRF fabric and the intermediate device.
  - Enable the IRF fabric to change its bridge MAC address as soon as the master leaves.
  - Create the ARP MAD VLAN and assign the ports on the ARP MAD links to the VLAN.

If the intermediate device is in an IRF fabric, assign this fabric a different domain ID than the ARP MAD-enabled fabric to avoid false detection of IRF split.

Examples

# Enable ARP MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad arp enable
```

mad enable

Syntax

mad enable

undo mad enable

View

Layer 2 aggregate interface view

Default level

3: Manage level

Parameters

None

Description

Use **mad enable** to enable LACP MAD.

Use **undo mad enable** to disable LACP MAD.

By default, LACP MAD is disabled.

LACP MAD uses extended LACP packets for detecting multi-active collisions and requires an intermediate HP device that also supports LACP MAD packets.

When you use LACP MAD, follow these guidelines:

- The intermediate device must be an HP device that support extended LACP for MAD.
- If the intermediate device is in an IRF fabric, assign this fabric a different domain ID than the LACP MAD-enabled fabric to avoid false detection of IRF partition.

- Use dynamic link aggregation mode. MAD is LACP dependent. Even though LACP MAD can be configured on both static and dynamic aggregate interfaces, it takes effect only on dynamic aggregate interfaces.
- Configure link aggregation settings also on the intermediate device.

Examples

# Enable LACP MAD on Bridge-Aggregation 1, a Layer 2 dynamic aggregate interface.

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

mad exclude interface

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

View

System view

Default level

3: Manage level

Parameters

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

Description

Use **mad exclude interface** to exclude a physical network port from being shut down when the IRF fabric transitions to the Recovery state upon detection of a multi-active collision.

Use **undo mad exclude interface** to restore the default MAD action on a physical network port.

By default, all physical network ports but the IRF physical ports shut down when the IRF fabric transitions to the Recovery state.

MAD action is not configurable for IRF physical ports.

When MAD detects that an IRF fabric has split into two or more identical active IRF fabrics, only the IRF fabric whose master has the lowest member ID among all the masters can still forward data traffic. MAD changes its status to Recovery on all the other IRF fabrics and shuts down all their physical ports except the IRF physical ports and those manually configured to not shut down.

If a port must be kept in up state for special purposes such as Telnet connection, exclude it from the shutdown action. To avoid problems, HP recommends excluding only the one used for Telnet for the management purpose.

The ports that have shut down by MAD come up when the member devices reboot to join the recovered IRF fabric. If auto recovery fails because the current master has failed or any other exception has occurred, use the **mad restore** command to manually recover the member devices and bring up the ports.

Examples

# Exclude GigabitEthernet 2/0/5 from being shut down when the MAD status transitions to Recovery.

```
<Sysname> system-view
[Sysname] mad exclude interface gigabitethernet 2/0/5
```

mad restore

Syntax

mad restore

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **mad restore** to restore the normal MAD state of the IRF fabric in Recovery state.

When MAD detects that an IRF fabric has split into multiple IRF fabrics, only the one whose master has the lowest member ID among all the masters can still forward traffic. All the other fabrics are set in Recovery state and cannot forward traffic.

If the active IRF fabric has failed before the IRF split problem is fixed, use this command to restore an IRF fabric in Recovery state to take over the active IRF fabric role.

Examples

# Restore the normal MAD state of the IRF fabric in Recovery state.

```
<Sysname> system-view
[Sysname] mad restore
   This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

port group interface

Syntax

port group interface *interface-type interface-number* [**mode** { **enhanced** | **normal** }]

undo port group interface *interface-name*

View

IRF port view

Default level

3: Manage level

Parameters

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

interface-name: Specifies a physical port in the *interface-typeinterface-number* format. No space is allowed between the *interface-type* and *interface-number* arguments.

mode: Sets the operating mode of the physical IRF port. If no mode is set, the port operates in enhanced mode. The operating mode set in this command takes effect only when the physical port is operating as an IRF physical port.

- **enhanced**—Sets the physical IRF port to operate in enhanced mode. The switch does not support this keyword.
- **normal**—Sets the physical IRF port to operate in normal mode. The switch does not support this keyword.

Description

Use **port group interface** to bind a physical port to an IRF port.

Use **undo port group interface** to remove the binding of a physical port and an IRF port.

By default, no physical ports are bound to any IRF port.

Before binding a physical port to an IRF port or removing their binding, use the **shutdown** command to shut down the physical port.

The switch supports up to two physical ports for an IRF port, and these two ports must be located on the same interface card.

Make sure the physical ports at both ends of an IRF link are using the same operating mode. For an aggregate IRF link, HP recommends configuring the same operating mode for all physical IRF ports at both ends.

The system does not automatically remove the binding between a physical port and an IRF port, even if the IRF link has been lost, for example, because the interface card holding the physical port is removed. To remove the binding, use the **undo port group interface** command.

Examples

# Bind Ten-GigabitEthernet 3/1/1 to IRF port 3/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/1/1
[Sysname-Ten-GigabitEthernet3/1/1] shutdown
[Sysname-Ten-GigabitEthernet3/1/1] quit
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/1/1
[Sysname-irf-port3/1] quit
[Sysname] interface ten-gigabitethernet 3/1/1
[Sysname-Ten-GigabitEthernet3/1/1] undo shutdown
```

Index

Contents

Ethernet interface configuration commands

broadcast-suppression

Syntax

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

undo broadcast-suppression

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

ratio: Sets the broadcast suppression threshold as a percentage of the transmission capability of an Ethernet interface, ranging from 1 to 100. The smaller the percentage, the less broadcast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of broadcast packets that the Ethernet interface can forward per second.

- For GE ports, the *max-pps* argument ranges from 1 to 1,488,100 pps.
- For 10-GE ports, the *max-pps* argument ranges from 1 to 14,881,000 pps.

kbps *max-kbps*: Specifies the maximum number of kilobits of broadcast traffic that the Ethernet interface can forward per second.

- For GE ports, the *max-kbps* argument ranges from 1 to 1,000,000 kbps.
- For 10-GE ports, the *max-kbps* argument ranges from 1 to 10,000,000 kbps.

Description

Use **broadcast-suppression** to set the broadcast suppression threshold on one or multiple Ethernet interfaces.

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

By default, Ethernet interfaces do not suppress broadcast traffic.

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

When broadcast traffic exceeds the broadcast suppression threshold, the system discards broadcast packets until the broadcast traffic drops below the threshold.

NOTE:

- If you set different broadcast suppression thresholds in Ethernet interface view or port group view multiple times, the one configured last takes effect.
- For a particular type of traffic, configure either storm suppression or storm control, but not both. If both of them are configured, you may fail to achieve the expected storm control effect.

Examples

# Set the broadcast suppression threshold to 20% on GigabitEthernet 1/0/1.

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

# Set the broadcast suppression threshold to 20% on all ports in the manual port group named group1.

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

default

Syntax

default

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

△ CAUTION:

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

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

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

Examples

# Restore the default settings for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Syntax

description *text*

undo description

View

Ethernet interface view

Default level

2: System level

Parameters

text: Specifies the interface description, a string of 1 to 80 characters. The string can include case-sensitive letters, digits, special characters such as tilde (~), exclamation point (!), at sign (@), pound sign (#), dollar sign ($), percent sign (%), caret (^), ampersand sign (&), asterisk (*), left brace({), right brace (}), left parenthesis ((), right parenthesis ()), left bracket ([), right bracket (]), left angle bracket (<), right angle bracket (>), hyphen (-), underscore(_), plus sign (+), equal sign (=), vertical bar (|), back slash (\), colon (:), semi-colon (;) quotation marks ("), apostrophe ('), comma (,), dot (.), and slash (/), spaces, and other Unicode characters and symbols.

When you specify a description, follow these guidelines:

- Each Unicode character takes the space of two regular characters.
- To use Unicode characters or symbols in an interface description, install the specific input method editor and log in to the switch through remote login software that supports the character type.
- When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.

Description

Use **description** to change the description of the interface.

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

The default description of an interface is the interface name plus **Interface**. For example, **GigabitEthernet1/0/1 Interface**.

Related commands: **display interface**.

Examples

# Change the description of interface GigabitEthernet 1/0/1 to **lanswitch-interface**.

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

display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Displays inbound traffic statistics.

outbound: Displays outbound traffic statistics.

interface-type: Specifies an interface type.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display counters** to display traffic statistics for interfaces.

- If an interface type is specified, this command displays traffic statistics for all interfaces of the specified type.
- If no interface type is specified, this command displays traffic statistics for all interfaces that have traffic counters.

Examples

# Display inbound traffic statistics for all GigabitEthernet interfaces.

```
<Sysname> display counters inbound interface gigabitethernet
Interface            Total(pkts)    Broadcast(pkts)    Multicast(pkts) Err(pkts)
GE1/0/1                        100                100                 0         0
GE1/0/2                          0                  0                 0         0
GE1/0/3                   Overflow           Overflow          Overflow  Overflow
GE1/0/4                          0                  0                 0         0

 Overflow: more than 14 decimal digits(7 digits for column "Err").
       --: not supported.
```

Table 1 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts)	Total number of packets received or sent through the interface.
Broadcast (pkts)	Total number of broadcast packets received or sent through the interface.
Multicast (pkts)	Total number of multicast packets received or sent through the interface.
Err (pkts)	Total number of error packets received or sent through the interface.

Field	Description
Overflow: more than 14 decimal digits(7 digits for column "Err").	The command displays **Overflow**, if any of the following applies: • The data length of an error statistic is greater than 7 decimal digits. • The data length of a non-error statistic is greater than 14 decimal digits.
--: not supported.	The statistical item is not supported.

display counters rate

Syntax

display counters rate { **inbound** \| **outbound** } **interface** [*interface-type*] [**\|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Displays inbound traffic rate statistics.

outbound: Displays outbound traffic rate statistics.

interface-type: Specifies an interface type.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display counters rate** to display traffic rate statistics over the last sampling interval.

The statistics cover only interfaces in up state. If an interface type is specified, the command displays traffic rate statistics for all up interfaces of the specified type. If no interface type is specified, the command displays traffic rate statistics for all up interfaces that have traffic counters.

To set the statistics polling interval, use the **flow-interval** command. The default statistics polling interval is five minutes.

Related commands: **flow-interval**.

Examples

# Display the inbound traffic rate statistics for all GigabitEthernet interfaces.

```
<Sysname> display counters rate inbound interface gigabitethernet
Interface           Total(pkts/sec)   Broadcast(pkts/sec)   Multicast(pkts/sec)
GE1/0/1                         0                    --                    --

 Overflow: more than 14 decimal digits.
```

```
        --: not supported.
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts/sec)	Average rate (in packets per second) of receiving or sending packets during the sampling interval.
Broadcast (pkts/sec)	Average rate (packets per second) of receiving or sending broadcast packets during the sampling interval.
Multicast (pkts/sec)	Average rate (packets per second) of receiving or sending multicast packets during the sampling interval.
Overflow: more than 14 decimal digits.	The command displays **Overflow**, if any of the following applies: • The data length of an error statistic is greater than 7 decimal digits. • The data length of a non-error statistic is greater than 14 decimal digits.
--: not supported.	The statistical item is not supported.

display interface

Syntax

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

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

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

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

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display interface** to display Ethernet interface information.

If no interface type is specified, this command displays information about all interfaces.

If an interface type is specified but no interface number is specified, this command displays information about all interfaces of that type.

Related commands: **interface**.

Examples

# Display detailed information about interface GigabitEthernet 1/0/1.

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2d2-58fb
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 1000Mbps-speed mode, unknown-duplex mode
 Link speed type is force link, link duplex type is autonegotiation
 Flow-control is enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Port priority: 0
 Last clearing of counters:  Never
 Peak value of input: 0 bytes/sec, at 2000-06-13 15:27:44
 Peak value of output: 0 bytes/sec, at 2000-06-13 15:27:44
 Last 300 seconds input:  0 packets/sec 0 bytes/sec 0%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec 0%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, - bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, - bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
```

```
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

Table 3 Command output

Field	Description
GigabitEthernet1/0/1 current state	Physical state of the Ethernet interface. For more information, see Table 4.
IP Packet Frame Type	Ethernet framing format on the interface.
Hardware address	Hardware address of the port.
Description	Description of the interface.
Loopback is not set	The loopback testing function is disabled.
Unknown-speed mode	The port speed is unknown.
unknown-duplex mode	The duplex mode is unknown.
Link speed type is autonegotiation	The interface will negotiate a speed with its peer.
link duplex type is autonegotiation	The interface will negotiate a duplex mode with its peer.
The Maximum Frame Length	Maximum Ethernet frame length allowed on the interface.
Broadcast MAX-ratio	Broadcast suppression threshold as a percentage of the interface transmission capability. When the threshold is exceeded, the interface drops broadcast packets.
Unicast MAX-ratio	Unknown unicast suppression threshold as a percentage of the interface transmission capability. When the threshold is exceeded, the interface drops unknown unicast packets.
Multicast MAX-ratio	Multicast suppression threshold as a percentage of the interface transmission capability. When the threshold is exceeded, the interface drops multicast packets.
Allow jumbo frame to pass	Maximum length of Ethernet frames that are allowed to pass through the interface.
PVID	Port VLAN ID.
Mdi type	Cable type.
Port link-type	Link type of the interface, which could be access, trunk, or hybrid.
Tagged VLAN ID	VLANs for which the interface sends packets without removing VLAN tags.
Untagged VLAN ID	VLANs for which the interface sends packets after removing VLAN tags.
Last clearing of counters: Never	Time when the **reset counters interface** command was last used to clear statistics on the interface. **Never** indicates that the **reset counters interface** command was never used since the switch was started.
Peak value of input	Peak value of inbound traffic, in Bps.
Peak value of output	Peak value of outbound traffic, in Bps.
Last 300 seconds input: 0 packets/sec 0 bytes/sec Last 300 seconds output: 0 packets/sec 0 bytes/sec	Average rate of input and output traffic in the last 300 seconds, in pps and Bps.

Field	Description
Input (total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	Inbound traffic statistics (in packets and bytes) for the interface. All inbound normal and abnormal packets (including unicast, broadcast, and multicast), and pause frames were counted.
Input (normal): 0 packets, - bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	Inbound traffic statistics (in packets and bytes) for the interface. All inbound normal packets (including unicast, broadcast, and multicast), and pause frames were counted.
input errors	Inbound packets with errors.
runts	Inbound frames shorter than 64 bytes, in correct format, and containing valid CRCs.
giants	Inbound frames larger than the maximum frame length supported on the interface. • For an Ethernet interface that does not permit jumbo frames, giants refer to frames larger than 1536 bytes (without VLAN tags) or 1540 bytes (with VLAN tags). • For an Ethernet interface that permits jumbo frames, giants refer to frames larger than the maximum length of Ethernet frames that are allowed to pass through, which is configured when you configure jumbo frame support on the interface.
- throttles	Number of times that the port shut down due to buffer or CPU overload.
frame	Total number of inbound frames that contained checksum errors and a non-integer number of bytes.
- overruns	Number of packet drops because the input rate of the port exceeded the queuing capability.
aborts	Total number of illegal inbound packets: • **Fragment frames**—CRC error frames shorter than 64 bytes. The length can be an integral or non-integral value. • **Jabber frames**—CRC error frames greater than the maximum frame length supported on the Ethernet interface (with an integral or non-integral length). For an Ethernet interface that does not permit jumbo frames, jabber frames refer to CRC error frames greater than 1518 bytes (without VLAN tags) or 1522 bytes (with VLAN tags). For an Ethernet interface that permits jumbo frames, jabber frames refer to CRC error frames greater than the maximum length of Ethernet frames that are allowed to pass through the interface (which is configured when you configure jumbo frame support on the interface). • **Symbol error frames**—Frames that contained at least one undefined symbol. • **Unknown operation code frames**—Non-pause MAC control frames • **Length error frames**—Frames whose 802.3 length fields did not accord with the actual frame length (46 to 1500 bytes).
ignored	Number of inbound frames dropped because the receive buffer of the port ran low.
- parity errors	Total number of frames with parity errors.

Field	Description
Output (total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	Outbound traffic statistics (in packets and bytes) for the port. All outbound normal and abnormal packets (including unicast, broadcast, and multicast), and pause frames were counted.
Output (normal): 0 packets, - bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	Outbound normal traffic (including unicast, broadcast, and multicast) and pause frame statistics (in packets and bytes) for the interface.
output errors	Outbound packets with errors.
- underruns	Number of packet drops because the output rate of the interface exceeded the output queuing capability. This is a low-probability hardware anomaly.
- buffer failures	Number of packets dropped because the transmit buffer of the interface ran low.
aborts	Number of packets that failed to be transmitted, for example, because of Ethernet collisions.
deferred	Number of frames that the interface deferred to transmit because of detected collisions.
collisions	Number of frames that the interface stopped transmitting because Ethernet collisions were detected during transmission.
late collisions	Number of frames that the interface deferred to transmit after transmitting their first 512 bits, because of detected collisions.
lost carrier	Number of carrier losses during transmission. This counter applies to serial WAN interfaces.
- no carrier	Number of times that the port failed to detect the carrier when attempting to send frames. This counter applies to serial WAN interfaces.

NOTE:

If an output field is not available, a hyphen (-) is displayed.

Table 4 Description on the possible physical states of a Ethernet interface

Field	Description
UP	The interface is physically up.
DOWN	The interface is physically down, because no physical connection exists. Possible reason: The network cable is disconnected or faulty.
DOWN (Administratively)	The interface is physically down, because it was shut down with the **shutdown** command. To restore its physical state, use the **undo shutdown** command.
DOWN (Link-Aggregation interface down)	The interface is physically down, because the aggregate interface corresponding to the aggregation group to which it belongs was shut down with the **shutdown** command.
DOWN (OAM connection failure)	The interface is physically down, because an OAM connection fails to be established on it or the OAM connection is disconnected.
DOWN (DLDP connection failure)	The interface is physically down, because a DLDP connection fails to be established on it or the DLDP connection is disconnected.

Field	Description
DOWN (Loopback detection-protected)	The interface is shut down, because a loop is detected on it.
DOWN (BPDU-protected)	The interface is shut down by the BPDU guard function.
DOWN (Monitor-Link uplink down)	The interface is physically down, because the uplink of the monitor link group to which it belongs is down.

# Display brief information about all interfaces.

```
<Sysname> display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                UP   UP(s)    --
Vlan1                UP   UP       192.168.0.85
Vlan2                DOWN DOWN     --
Vlan1010             DOWN DOWN     --

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                DOWN auto    A      A    1
GE1/0/1              DOWN 1G      A      A    1
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              DOWN auto    A      A    1
GE1/0/4              DOWN auto    A      A    1
GE1/0/5              DOWN auto    A      A    1
GE1/0/6              DOWN auto    A      A    1
GE1/0/7              DOWN auto    A      A    1
GE1/0/8              DOWN auto    A      A    1
GE1/0/9              DOWN auto    A      A    1
GE1/0/10             DOWN auto    A      A    1
```

# Filter the brief interface information to display the line starting with the **(s)** string and all subsequent lines.

```
<Sysname>display interface brief | begin (s)
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                UP   UP(s)    --
RAGG1                DOWN DOWN     --
Vlan1                UP   UP       192.168.0.55
Vlan2                DOWN DOWN     --
```

When you use the **begin** keyword to filter the output, the system only searches the Layer 3 interface list or the Layer 2 interface list. If *regular-expression* is on the Layer 3 interface list, the system only displays the line that contains *regular-expression,* and all subsequent lines on the Layer 3 interface list.

```
<Sysname> display interface brief down
The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
BAGG1                DOWN Not connected
GE1/0/1              DOWN Not connected
GE1/0/2              DOWN Not connected
GE1/0/4              DOWN Not connected
GE1/0/5              DOWN Not connected
```

Table 5 Command output

Field	Description
The brief information of interface(s) under route mode:	The command displays brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link layer state of the interface: • **ADM**—The interface has been shut down by the network administrator. To recover its physical layer state, perform the **undo shutdown** command. • **Stby**—The interface is a standby interface.
Protocol: (s) - spoofing	If the network layer protocol state of an interface is shown as UP, but its link is an on-demand link or not present at all, its protocol attribute includes the spoofing flag (an **s** in parentheses). This attribute is typical of interface Null 0 and the loopback interfaces.
Interface	Interface name.
Link	Physical link state of the interface: • **UP**—The link is up. • **DOWN**—The link is physically down. • **ADM**—The link has been administratively shut down. To recover its physical state, perform the **undo shutdown** command. • **Stby**—The interface is a standby interface.
Protocol	Protocol connection state of the interface, which can be UP, DOWN, or UP(s).
The brief information of interface(s) under bridge mode:	Brief information about Layer 2 interfaces.
Speed or Duplex: (a)/A - auto; H - half; F - full	If the speed of an interface is automatically negotiated, its speed attribute includes the auto negotiation flag, letter a in parentheses. If the duplex mode of an interface is automatically negotiated, its duplex mode attribute includes the following options: • **(a)/A**—Auto negotiation • **H**—Half negotiation • **F**—Full negotiation
Type: A - access; T - trunk; H – hybrid	Link type options for Ethernet interfaces.
Speed	Interface rate, in bps.

Field	Description
Duplex	Duplex mode of the interface: - **A**—Auto-negotiation - **F**—Full duplex - **F(a)**—Auto-negotiated full duplex - **H**—Half duplex - **H(a)**—Auto-negotiated half duplex
Type	Link type of the interface: - **A**—Access - **H**—Hybrid - **T**—Trunk
PVID	Port VLAN ID of the interface.
Cause	Causes for the physical state of an interface to be DOWN. For more information, see Table 6.

Table 6 Causes for the physical state of an interface to be DOWN

Field	Description
Not connected	No physical connection exists (possibly because the network cable is disconnected or faulty).
Administratively	The port was shut down with the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.
Link-Aggregation interface down	The aggregate interface corresponding to the aggregation group to which the interface belongs was shut down with the **shutdown** command.
OAM connection failure	OAM connection fails (possibly because the connection fails to be established or the connection is disconnected).
DLDP connection failure	DLDP connection fails (possibly because the connection fails to be established or the connection is disconnected).
Loopback detection-protected	The interface is shut down because a loop is detected on it.
BPDU-protected	The interface is shut down by the BPDU guard function.
Monitor-Link uplink down	The uplink of the monitor link group to which the interface belongs is down.

display loopback-detection

Syntax

display loopback-detection [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display loopback-detection** to display the status of the loopback detection function.

If loopback detection is enabled, this command also displays the detection interval and ports in a loop condition.

Examples

# Display information about loopback detection.

```
<Sysname> display loopback-detection
 Loopback detection is running.
 Loopback detection is in multi-port mode.
 Detection interval is 30 seconds.
 No port is detected with loopback.
```

Table 7 Command output

Field	Description
Loopback-detection is in multi-port mode.	Multi-port loopback detection is enabled. This field appears only when the switch supports the **loopback-detection multi-port-mode enable** command.
Detection interval time is 30 seconds.	Loopback detection interval is 30 seconds.
No port is detected with loopback.	No loops are detected on ports.

display packet-drop interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

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

Examples

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

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

Table 8 Command output

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

display packet-drop summary

Syntax

display packet-drop summary [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

# Display information about dropped packets on all interfaces.

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

For the description of some fields in the output, seeTable 8.

display port combo

Syntax

display port combo [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case-sensitive string of 1 to 256 characters.

Description

Use **display port combo** to display the combo interfaces of the switch and the fiber and copper combo ports.

Examples

# Display the combo interfaces of the switch and the fiber and copper combo ports.

```
<Sysname> display port combo
Combo-group         Active                      Inactive
       1         GigabitEthernet1/0/46       GigabitEthernet1/0/49
       2         GigabitEthernet1/0/47       GigabitEthernet1/0/52
       3         GigabitEthernet1/0/48       GigabitEthernet1/0/50
       4         GigabitEthernet1/0/51       GigabitEthernet1/0/45
```

Table 9 Command output

Field	Description
Combo-group	Combo interfaces of the switch, represented by combo interface numbers that are generated by the system.
Active	Ports of the combo interfaces that are active.
Inactive	Ports of the combo interfaces that are inactive.

In a combo interface, the fiber or copper combo port with the smaller port number is active by default. You can determine whether a port is a fiber combo port or a copper combo port by checking the "Media type is" field of the **display interface** command.

display port-group manual

Syntax

display port-group manual [**all** | **name** *port-group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

all: Displays information about all port groups.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-group manual** to display information about port groups.

If the **all** keyword is specified, this command displays the name and member Ethernet interfaces of each port group on the switch.

If a port group is specified, this command displays its name and member Ethernet interfaces.

If you do not specify the **all** keyword or any port group name, the command displays the name of each port group on the switch.

Examples

# Display the names of all port groups.

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

```
group1                                    group2
```

# Display detailed information about all port groups.

```
<Sysname> display port-group manual all
Member of group1:
    GigabitEthernet1/0/3          GigabitEthernet1/0/4          GigabitEthernet1/0/5
    GigabitEthernet1/0/6          GigabitEthernet1/0/7

Member of group2:
None
```

# Display detailed information about the port group named group1.

```
<Sysname> display port-group manual name group1
Member of group1:
    GigabitEthernet1/0/3          GigabitEthernet1/0/4          GigabitEthernet1/0/5
    GigabitEthernet1/0/6          GigabitEthernet1/0/7
```

display storm-constrain

Syntax

display storm-constrain [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

broadcast: Displays broadcast storm control settings and statistics.

multicast: Displays multicast storm control settings and statistics.

unicast: Displays unknown unicast storm control settings and statistics.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display storm-constrain** to display storm control settings and statistics.

If you specify no argument or keyword, this command displays all storm control settings on all storm control-enabled interfaces.

When the port forwarding state transition counter (Swi-num) reaches 65535, it automatically wraps back to 0.

Examples

# Display the storm control settings on all storm control-enabled ports.

```
<Sysname> display storm-constrain
Abbreviation: BC - broadcast; MC - multicast; UC - unicast
 Flow Statistic Interval: 10(second)
PortName      Type LowerLimit UpperLimit CtrMode  Status  Trap Log SwiNum Unit
------------------------------------------------------------------------------
GE1/0/30      MC   100        200        N/A      normal  on   on  0      kbps
```

Table 10 Command output

Field	Description
Flow Statistic Interval	Traffic polling interval of the storm control module.
PortName	Abbreviated port name.
StormType	Type of traffic subjected to storm control. Options include broadcast, multicast and unknown unicast.
LowerLimit	Lower storm control threshold, in pps, kbps, or percentage.
UpperLimit	Upper storm control threshold, in pps, kbps, or percentage.
Ctrmode	Protective action (block or shutdown) taken on the port when the upper threshold is reached. If you have not configured any protective action, N/A is displayed.
Status	Packet forwarding status: • **Normal**—The port is forwarding traffic normally. • **Control**—The port is in controlled mode.
Trap	Status of the storm control threshold event trap switch: • **On**—The port sends threshold event traps. • **Off**—The port does not send threshold event traps.
Log	Status of the storm control threshold event log switch: • **On**—The port sends threshold event log messages. • **Off**—The port does not send threshold event log messages.
Swi-num	Number of times the forwarding state of the interface changes. When the **Swi-num** count reaches 65,535, it resets automatically.

duplex

Syntax

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

undo duplex

View

Ethernet interface view

Default level

2: System level

Parameters

auto: Sets the interface to operate in auto-negotiation mode.

full: Sets the interface to operate in full duplex mode.

half: Sets the interface to operate in half-duplex mode. This keyword is not available for Ethernet copper ports that are configured with a 1000-Mbps port speed and fiber ports.

Description

Use **duplex** to set the duplex mode for an Ethernet interface.

Use **undo duplex** to restore the default duplex mode of the Ethernet interface.

By default, Ethernet interfaces operate in auto-negotiation mode.

Related commands: **speed**.

Examples

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

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

flow-control

Syntax

flow-control

undo flow-control

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **flow-control** to enable TxRx mode generic flow control on an Ethernet interface.

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

TxRx mode flow control enables an Ethernet interface to receive common pause frames from its peer, and send common pause frames to notify its peer of congestions.

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

With the **flow-control** command configured, an interface can both send and receive flow control frames:

- When congested, the interface sends a flow control frame to its peer.
- Upon receiving a flow control frame from the peer, the interface suspends sending packets.

To implement flow control on a link, you must enable the generic flow control function at both ends of the link.

Examples

# Enable TxRx mode generic flow control on the interface GigabitEthernet1/0/1.

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

flow-control receive enable

Syntax

flow-control receive enable

undo flow-control

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **flow-control receive enable** to enable Rx mode generic flow control on an Ethernet port.

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

Rx mode generic flow control enables an Ethernet interface to receive and process common pause frames from its peer. The interface does not send common pause frames when it is congested.

By default, Rx flow control is disabled on Ethernet interfaces.

With the **flow-control receive enable** command configured, an interface can receive, but not send flow control frames. When the interface receives a flow control frame from its peer, it suspends sending packets to the peer. When traffic congestion occurs on the interface, it cannot send flow control frames to the peer.

To handle unidirectional traffic congestion on a link, configure the **flow-control receive enable** command at one end, and the **flow-control** command at the other. To enable both ends of the link to handle traffic congestion, configure the **flow-control** command at both ends.

Examples

# Enable Rx mode generic flow control on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control receive enable
```

flow-interval

Syntax

flow-interval *interval*

undo flow-interval

View

Ethernet interface view

Default level

2: System level

Parameters

interval: Sets the statistics polling interval, in seconds. It ranges from 5 to 300 and must be a multiple of 5.

Description

Use **flow-interval** to set the interface statistics polling interval.

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

In system view, use the **flow-interval** command to set the statistics polling interval for all interfaces.

In Ethernet interface view, use the **flow-interval** command to set the statistics polling interval for the interface.

Examples

# Set the statistics polling interval to 100 seconds on GigabitEthernet 1/0/1.

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

group-member

Syntax

group-member *interface-list*

undo group-member *interface-list*

View

Port group view

Default level

2: System level

Parameters

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

Description

Use **group-member** to assign Ethernet interfaces to a port group.

Use **undo group-member** to remove Ethernet interfaces from the port group.

By default, a port group does not contain any member ports.

If you use the **group-member** *interface-type interface-start-number* **to** *interface-type interface-end-number* command to add multiple ports in batch to the specified port group, make sure that the *interface-end-number* argument must be greater than the *interface-start-number* argument.

Examples

# Assign Ethernet interface GigabitEthernet 1/0/1 to the port group named group1.

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

interface

Syntax

interface *interface-type interface-number*

View

System view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface type and number.

Description

Use **interface** to enter interface view.

Examples

# Enter GigabitEthernet 1/0/1 interface view (assuming that the interface is an Ethernet interface).

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

jumboframe enable

Syntax

jumboframe enable [*value*]

undo jumboframe enable

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

value: Sets the maximum length of Ethernet frames that are allowed to pass through, ranging from 1536 to 9216 bytes. If you set the *value* argument multiple times, the latest configuration takes effect.

Description

Use **jumboframe enable** to allow jumbo frames within the specified length to pass through one or multiple Ethernet interfaces.

Use **undo jumboframe enable** to prevent jumbo frames from passing through one or multiple Ethernet interfaces.

By default, the switch allows jumbo frames within 9216 bytes to pass through Ethernet interfaces.

In Ethernet interface view, the command applies only to the current Ethernet interface.

In port group view, the command applies to every Ethernet interface in the port group.

Examples

# Configure the switch to allow jumbo frames within 9216 bytes to pass through GigabitEthernet 1/0/1.

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

link-delay

Syntax

link-delay *delay-time*

undo link-delay

View

Ethernet interface view

Default level

2: System level

Parameters

delay-time: Sets the physical state change suppression interval on the Ethernet interface, ranging from 2 to 10 seconds.

Description

Use **link-delay** to set the physical state change suppression interval on an Ethernet interface.

Use **undo link-delay** to restore the default.

By default, the physical state change suppression interval on an Ethernet interface is 0 seconds.

Do not use this command on Ethernet interfaces with RRPP, MSTP, or Smart Link enabled.

NOTE:

This command does not apply to ports that are administratively shut down (with the **shutdown** command).

Examples

# Enable physical state change suppression on GigabitEthernet 1/0/1, setting the suppression interval to 8 seconds.

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

link-delay mode up

Syntax

link-delay *delay-time* **mode up**

undo link-delay

View

Ethernet interface view

Default level

2: System level

Parameters

delay-time: Sets the link down suppression interval, ranging from 2 to 10 seconds.

Description

Use **link-delay** *delay-time* **mode up** to enable an Ethernet interface to suppress link down events. When the physical link of the interface goes down, the interface suppresses the link down event and starts a timer. When the timer expires, the physical layer reports the event to the upper layers.

Use **undo link-delay** to restore the default.

By default, the link down suppression interval on an Ethernet interface is 0 seconds.

The **link-delay mode up** command and the **link-delay** command supersede each other. The command that is configured last takes effect.

Do not configure this command on ports with RRPP, MSTP, or Smart Link enabled.

Examples

# Enable link down suppression on GigabitEthernet 1/0/1, setting the suppression interval to 10 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay 10 mode up
```

loopback

Syntax

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

View

Ethernet interface view

Default level

2: System level

Parameters

external: Enables external loopback testing to test all on-chip functions related to Ethernet interfaces.

internal: Enables internal loopback testing to test the hardware of Ethernet interfaces.

Description

Use **loopback** to enable loopback testing on an Ethernet interface.

By default, loopback testing is disabled on Ethernet interfaces.

Enable loopback testing for troubleshooting purposes, such as identifying an Ethernet problem.

During loopback testing, the **speed**, **duplex**, **mdi**, and **shutdown** commands are not available. In addition, the port is operating in full duplex mode, regardless of its duplex configuration. After loopback testing is disabled, the duplex configuration of the port is restored.

Loopback testing is a one-time operation, and is not recorded in the configuration file.

Examples

# Enable internal loopback testing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
 Loop internal succeeded!
```

loopback-detection action

Syntax

loopback-detection action { **no-learning** | **semi-block** | **shutdown** }

undo loopback-detection action

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

no-learning: Disables MAC address learning on the interface.

semi-block: Blocks all packets but STP BPDUs, and disables MAC address learning on the interface.

shutdown: Shuts down the Ethernet interface. To bring up the interface again, use the **undo shutdown** command.

Description

Use **loopback-detection action** to configure the action for loop protection on Ethernet interfaces.

Use **undo loopback-detection action** to restore the default.

By default, a looped interface does not receive or send packets; the system generates traps and log messages, and deletes the MAC address table entries of the looped interface.

When you change the link type of an Ethernet interface by using the **port link-type** command, the switch removes the protective action configured on the interface. For more information about the **port link-type** command, see "VLAN configuration commands."

Examples

# Configure the access port GigabitEthernet 1/0/1 to shut down when a loop is detected.

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

# Configure the trunk port GigabitEthernet 1/0/2 to shut down when a loop is detected.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type trunk
```

```
[Sysname-GigabitEthernet1/0/2] loopback-detection enable
[Sysname-GigabitEthernet1/0/2] loopback-detection control enable
[Sysname-GigabitEthernet1/0/2] loopback-detection action shutdown
```

loopback-detection control enable

Syntax

loopback-detection control enable

undo loopback-detection control enable

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **loopback-detection control enable** to enable loopback detection control on trunk or hybrid ports.

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

By default, loopback detection control is disabled on trunk and hybrid ports.

When a hybrid or trunk port detects a loop condition, it sends traps, whether loopback detection control is enabled or not. However, only after loopback detection control is enabled will the port perform the protective action configured with the **loopback-detection action** command.

This command is not applicable to access ports.

Examples

# Enable loopback detection control on the trunk port GigabitEthernet 1/0/1.

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

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

System view, Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **loopback-detection enable** to enable loopback detection globally in system view or on interfaces in Ethernet interface or port group view. To use loopback detection on an Ethernet interface, you must enable the function both globally and on the port.

Use **undo loopback-detection enable** to disable loopback detection globally or on Ethernet interfaces.

The **undo loopback-detection enable** command in system view disables loopback detection on all interfaces.

By default, loopback detection is disabled on all Ethernet interfaces.

If an interface receives a packet that it sent out, a loop has occurred. Loops may cause broadcast storms, which degrade network performance. You can enable loopback detection to detect loops on an interface and, if the interface supports the **loopback-detection action** command, configure the protective action (shut down the port, for example) to take on the interface when a loop is detected.

In addition to the configured protective action, the switch also performs other actions to alleviate the impact of the loop condition. For more information, see Table 11.

Table 11 Actions to take upon detection of a loop condition

Port type	Actions	
	No protective action is configured	**A protective action is configured**
Access port	• Place the interface in controlled mode. The interface does not receive or send packets. • Generate traps. • Delete all MAC address entries of the interface.	• Perform the configured protective action. • Generate traps and log messages. • Delete all MAC address entries of the interface.
Hybrid or trunk port	• Generate traps. • If loopback detection control is enabled, set the interface in controlled mode. The interface does not receive or send packets. • Delete all MAC address entries of the interface.	• Generate traps and log messages. • If loopback detection control is enabled, take the configured protective action on the interface. • Delete all MAC address entries of the interface.

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

Examples

# Enable loopback detection on GigabitEthernet 1/0/1.

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

loopback-detection interval-time

Syntax

loopback-detection interval-time *time*

undo loopback-detection interval-time

View

System view

Default level

2: System level

Parameters

time: Sets the loopback detection interval, ranging from 5 to 300 seconds.

Description

Use **loopback-detection interval-time** to set the loopback detection interval.

Use **undo loopback-detection interval-time** to restore the default loopback detection interval.

The default loopback detection interval is 30 seconds.

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

Examples

# Set the loopback detection interval to 10 seconds.

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

loopback-detection multi-port-mode enable

Syntax

loopback-detection multi-port-mode enable

undo loopback-detection multi-port-mode enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **loopback-detection multi-port-mode enable** to enable multi-port loopback detection.

Use **undo loopback-detection multi-port-mode enable** to restore the default.

By default, multi-port loopback detection is disabled.

When detecting a loop between two interfaces, the switch takes the following actions on the looped interface:

- If the looped interface is an access interface, the switch performs the configured protective action, sends traps to the terminals, and deletes all MAC address entries of the interface.
- If the looped interface is a trunk or hybrid interface, the switch sends traps to the terminals. If loopback detection control is enabled, the switch performs the configured protection action on the looped interface and deletes all MAC address entries of the interface.

NOTE:

To enable multi-port loopback detection, you must configure the **loopback-detection multi-port-mode enable** and **loopback-detection enable** commands in system view, and configure the **loopback-detection enable** command in the view of the related interfaces.

Examples

# Enable multi-port loopback detection to monitor loops between GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] loopback-detection multi-port-mode enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] loopback-detection enable
```

loopback-detection per-vlan enable

Syntax

loopback-detection per-vlan enable

undo loopback-detection per-vlan enable

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **loopback-detection per-vlan enable** to enable loopback detection in each VLAN on trunk or hybrid ports.

Use **undo loopback-detection per-vlan enable** to disable loopback detection in all but the PVID on trunk or hybrid ports.

By default, a trunk port or hybrid port performs loopback detection only in its PVID.

The **loopback-detection per-vlan enable** command is not applicable to access ports.

Examples

# Enable loopback detection in all VLANs on hybrid port GigabitEthernet 1/0/1.

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

mdi

Syntax

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

undo mdi

View

Ethernet interface view

Default level

2: System level

Parameters

across: Sets the MDI mode to across. In this mode, pins 1 and 2 of the port are receive pins, and pins 3 and 6 are transmit pins.

auto: Sets the MDI mode to auto. In this mode, the port negotiates pin roles with its peer.

normal: Sets the MDI mode to normal. In normal mode, pins 1 and 2 of the port are transmit pins, and pins 3 and 6 are receive pins.

Description

Use **mdi** to configure the MDI mode of a copper Ethernet interface.

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

By default, Ethernet interfaces operate in auto MDI mode.

NOTE:

This command is not applicable to fiber ports.

Examples

# Set GigabitEthernet 1/0/1 to operate in across MDI mode.

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

multicast-suppression

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

undo multicast-suppression

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

ratio: Sets the multicast suppression threshold as a percentage of the transmission capability of an Ethernet interface, ranging from 1 to 100. The smaller the percentage, the less multicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of multicast packets that the Ethernet interface can forward per second.

- For GE ports, the *max-pps* argument ranges from 1 to 1,488,100 pps.
- For 10-GE ports, the *max-pps* argument ranges from 1 to 14,881,000 pps.

kbps *max-kbps*: Specifies the maximum number of kilobits of multicast traffic that the Ethernet interface can forward per second.

- For GE ports, the *max-kbps* argument ranges from 1 to 1,000,000 kbps.
- For 10-GE ports, the *max-kbps* argument ranges from 1 to 10,000,000 kbps.

Description

Use **multicast-suppression** to set the multicast suppression threshold on one or multiple Ethernet interfaces.

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

By default, Ethernet interfaces do not suppress multicast traffic.

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

When multicast traffic exceeds the threshold you configure, the system discards multicast packets until the multicast traffic drops below the threshold.

NOTE:

- If you set different multicast suppression thresholds in Ethernet interface view or port group view multiple times, the one configured last takes effect.
- For a particular type of traffic, configure either storm suppression or storm control, but not both. If both of them are configured, you may fail to achieve the expected storm control effect.

Examples

# Set the multicast threshold to 20% on GigabitEthernet 1/0/1.

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

# Set the multicast threshold to 20% on all ports in the port group named group1.

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

port auto-power-down

Syntax

port auto-power-down

undo port auto-power-down

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **port auto-power-down** to enable auto power-down on Ethernet interfaces for energy efficiency.

Use **undo port auto-power-down** to restore the default.

By default, auto power-down is disabled on Ethernet interfaces.

Examples

# Enable auto power-down on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port auto-power-down
```

# Enable auto power-down on all member ports of port group **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member gigabitethernet 1/0/1
[Sysname-port-group-manual-group1] group-member gigabitethernet 1/0/2
[Sysname-port-group-manual-group1] port auto-power-down
```

port bridge enable

Syntax

port bridge enable

undo port bridge enable

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port bridge enable** to enable bridging on a Ethernet interface.

Use **undo port bridge enable** to disable bridging on the Ethernet interface.

By default, bridging is not enabled on Ethernet interfaces.

Examples

# Enable bridging on Ethernet interface GigabitEthernet 1/0/1.

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port bridge enable
```

port-group manual

Syntax

port-group manual *port-group-name*

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

View

System view

Default level

2: System level

Parameters

port-group-name: Sets the port group name, a string of 1 to 32 characters.

Description

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

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

By default, no port group exists.

Examples

# Create port group **group1**.

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

reset counters interface

Syntax

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

View

User view

Default level

2: System level

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Description

Use **reset counters interface** to clear the Ethernet interface statistics.

Before collecting traffic statistics for a specific period of time on an interface, clear the old statistics first.

- If no interface type is specified, this command clears statistics for all interfaces.
- If only the interface type is specified, this command clears statistics for all interfaces of that type.

Examples

# Clear the statistics of GigabitEthernet 1/0/1.

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

reset packet-drop interface

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface-type: Specify an interface type.

interface-number: Specify an interface number.

Description

Use **reset packet-drop interface** to clear statistics of dropped packets on an interface or multiple interfaces.

Sometimes you need to clear the old statistics before you can collect statistics of dropped packets.

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

Examples

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

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

# Clear statistics of dropped packets on all interfaces.

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

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

△ CAUTION:

After you shut down an Ethernet interface with this command, it cannot forward packets, even if it is physically connected.

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

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

By default, an Ethernet interface is in up state.

Examples

# Shut down and then bring up GigabitEthernet 1/0/1.

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

# Shut down all member ports in the port group named group1.

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

speed

Syntax

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

undo speed

View

Ethernet interface view

Default level

2: System level

Parameters

10: Sets the interface speed to 10 Mbps.

100: Sets the interface speed to 100 Mbps.

1000: Sets the interface speed to 1000 Mbps.

auto: Enables the interface to negotiate a speed with its peer.

Description

Use **speed** to set the speed of an Ethernet interface.

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

By default, an Ethernet interface automatically negotiates a speed with the peer.

For an Ethernet copper port, use the **speed** command to set its speed to match the speed of the peer interface.

For a fiber port, use the **speed** command to set its speed to match the rate of a pluggable transceiver.

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

NOTE:

A Gigabit fiber port does not support the **10** or **100** keyword. A 10-Gigabit fiber port does not support this command.

Examples

# Configure GigabitEthernet 1/0/1 to operate at 100 Mbps.

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

speed auto

Syntax

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

undo speed

View

GE interface view

Default level

2: System level

Parameters

10: Sets 10 Mbps as an option for speed auto negotiation.

100: Sets 100 Mbps as an option for speed auto negotiation.

1000: Sets 1000 Mbps as an option for speed auto negotiation.

Description

Use **speed auto** to set options for speed auto negotiation.

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

By default, an Ethernet interface automatically negotiates a speed with the peer.

The **speed** command and the **speed auto** command supersede each other. The command that is configured last takes effect.

If you configure **speed 100** after configuring **speed auto 100 1000** on an interface, the interface speed is set to 100 Mbps by force without negotiation. If you configure **speed auto 100 1000** after configuring **speed 100** on the interface, the interface negotiates with its peer, and the negotiated speed is either 100 Mbps or 1000 Mbps.

To avoid negotiation failure, make sure that at least one speed option is supported at both ends.

NOTE:

This feature is supported only on Gigabit copper ports that support speed auto negotiation.

Examples

# Configure the port GigabitEthernet 1/0/1 to use 10 Mbps and 1000 Mbps for speed negotiation.

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

storm-constrain

Syntax

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

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

View

Ethernet interface view

Default level

2: System level

Parameters

all: Disables storm control for all types of packets: broadcast, multicast, and unknown unicast.

broadcast: Enables or disables broadcast storm control.

multicast: Enables or disables multicast storm control.

unicast: Enables or disables unknown unicast storm control.

pps: Sets storm control thresholds in pps.

kbps: Sets storm control thresholds in kbps.

ratio: Sets storm control thresholds as a percentage of the transmission capacity of the interface.

max-values: Sets the upper threshold.

min-values: Sets the lower threshold, ranging from 1 to *max-values*.

Description

Use **storm-constrain** to enable broadcast, multicast, or unknown unicast storm control on an Ethernet port.

Use **undo storm-constrain** to disable storm control.

By default, traffic storm control is disabled.

To achieve desirable storm protection effect, avoid configuring both the **storm-constrain** command and any storm suppression command (**unicast-suppression**, **multicast-suppression**, and **broadcast-suppression**) on a port.

An upper threshold must be greater than or equal to the corresponding lower threshold. HP does not recommend configuring the same value for the two thresholds.

Examples

# Enable unknown unicast storm control on GigabitEthernet 1/0/1, setting the upper and lower thresholds to 200 pps and 150 pps.

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain unicast pps 200 150
```

# Enable broadcast storm control on GigabitEthernet 1/0/2, setting the upper and lower thresholds to 2000 kbps and 1500 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] storm-constrain broadcast kbps 2000 1500
```

# Enable multicast storm control on GigabitEthernet 1/0/3, setting the upper and lower thresholds to 80% and 15%.

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

storm-constrain control

Syntax

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

undo storm-constrain control

View

Ethernet interface view

Default level

2: System level

Parameters

block: Blocks this type of traffic, while forwarding other types of traffic. Even though the interface does not forward the blocked traffic, it still counts the traffic. When the blocked traffic is detected dropping below the lower threshold, the port begins to forward the traffic.

shutdown: Shuts down automatically. The interface shuts down automatically and stops forwarding any traffic. When the blocked traffic is detected dropping below the lower threshold, the port does not forward the traffic. To bring up the interface, perform the **undo shutdown** command or disable the storm control function.

Description

Use **storm-constrain control** to set the protective action to take on an Ethernet interface when a type of traffic (unknown unicast, multicast, or broadcast) exceeds the upper storm control threshold.

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

By default, no action is taken on an Ethernet interface when a type of traffic exceeds the upper storm control threshold.

Examples

# Configure GigabitEthernet 1/0/1 to block the traffic detected crossing the upper storm control threshold.

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

storm-constrain enable log

Syntax

storm-constrain enable log

undo storm-constrain enable log

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **storm-constrain enable log** to enable an Ethernet interface to log storm control threshold events. Logged events include traffic exceeding the upper threshold and traffic falling below the lower threshold from the upper threshold.

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

By default, a storm control-enabled port sends log messages when monitored traffic exceeds the upper threshold or falls below the lower threshold from the upper threshold.

Examples

# Disable GigabitEthernet 1/0/1 from sending out log messages upon detecting storm control threshold events.

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

storm-constrain enable trap

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **storm-constrain enable trap** to enable an Ethernet interface to send storm control threshold event traps. Triggering events include traffic exceeding the upper threshold and traffic falling below the lower threshold from the upper threshold.

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

By default, a storm control-enabled interface sends traps when monitored traffic exceeds the upper threshold or falls below the lower threshold from the upper threshold.

Examples

# Disable GigabitEthernet 1/0/1 from sending out storm control threshold event traps.

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

storm-constrain interval

Syntax

storm-constrain interval *seconds*

undo storm-constrain interval

View

System view

Default level

2: System level

Parameters

seconds: Sets the traffic polling interval of the storm control module, ranging from 1 to 300 seconds.

Description

Use **storm-constrain interval** to set the traffic polling interval of the storm control module.

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

By default, the storm control module polls traffic statistics every 10 seconds.

For network stability, use the default or a higher polling interval.

NOTE:

The interval set by the **storm-constrain interval** command is specific to storm control. To set the statistics polling interval of an interface, use the **flow-interval** command.

Examples

# Set the traffic statistics polling interval of the storm control module to 60 seconds.

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

unicast-suppression

Syntax

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

undo unicast-suppression

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

ratio: Sets the unknown unicast suppression threshold as a percentage of the transmission capability of an Ethernet interface, ranging from 1 to 100. The smaller the percentage, the less unknown unicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of unknown unicast packets that the Ethernet interface can forward per second.

- For GE ports, the *max-pps* argument ranges from 1 to 1,488,100 pps.
- For 10-GE ports, the *max-pps* argument ranges from 1 to 14,881,000 pps.

kbps *max-kbps*: Specifies the maximum number of kilobits of unknown unicast traffic that the Ethernet interface can forward per second.

- For GE ports, the *max-kbps* argument ranges from 1 to 1,000,000 kbps.
- For 10-GE ports, the *max-kbps* argument ranges from 1 to 10,000,000 kbps.

Description

Use **unicast-suppression** to set the unknown unicast suppression threshold on one or multiple Ethernet interfaces.

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

By default, Ethernet interfaces do not suppress unknown unicast traffic.

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

When unknown unicast traffic exceeds the threshold you configure, the system discards unknown unicast packets until the unknown unicast traffic drops below the threshold.

NOTE:

- If you set different unknown unicast suppression thresholds in Ethernet interface view or port group view multiple times, the one configured last takes effect.
- For a particular type of traffic, configure either storm suppression or storm control, but not both. If both of them are configured, you may fail to achieve the expected storm control effect.

Examples

# Set the unknown unicast threshold to 20% on GigabitEthernet 1/0/1.

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

# Set the unknown unicast threshold to 20% on all ports of port group **group1**.

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

virtual-cable-test

Syntax

virtual-cable-test

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **virtual-cable-test** to test the cable connection of an Ethernet interface. The test results are displayed within five seconds.

The following cable states are available:

- Normal—The cable is in good condition.
- Abnormal—Any fault other than a short or open circuit is detected.

If the cable connection is normal, the displayed cable length is the total length of the cable.

If the cable connection has a fault, it is the length from the local port to the faulty point.

If the link of an Ethernet interface is up, testing its cable connection will cause the link to go down and then up.

The test result is for reference only. The cable length detection error is up to 5 m (about 16 ft). If a test item is not available, a hyphen (-) is displayed.

NOTE:

Fiber ports do not support this command.

Examples

# Test the cable connection of GigabitEthernet 1/0/1.

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

NOTE:

The **Pair Impedance mismatch** field has the following values:

- **Yes**—Match
- **No**—Mismatch

Loopback and null interface configuration commands

default

Syntax

default

View

Loopback interface view, null interface view

Default level

2: System level

Parameters

None

Description

Use **default** to restore the default settings for the loopback or null interface.

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

△ CAUTION:

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

Examples

# Restore the default settings of interface loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-loopback0] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Syntax

description *text*

undo description

View

Loopback interface view, null interface view

Default level

2: System level

Parameters

text: Creates an interface description, a string of 1 to 80 characters. Valid characters and symbols include English letters (A to Z, a to z), digits (0 to 9), special English characters, spaces, and other Unicode characters and symbols.

Description

Use **description** to set a description for the interface.

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

By default, the description of a loopback or null interface is *interface name* Interface. For example: Loopback0 interface.

An interface description can be a mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.

To use a type of Unicode characters or symbols in an interface description, you must install the corresponding Input Method Editor (IME) and log in to the device through supported remote login software.

Each non-English Unicode character or symbol takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line. If a line is broken, it may break a Unicode character into two parts and create garbled characters.

Related commands: **display interface**.

Examples

# Set the description for interface loopback 0 to loopback0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-loopback0] description loopback0
```

display interface loopback

Syntax

display interface [**loopback**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

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

View

Any view

Default level

1: Monitor level

Parameters

interface-number: Loopback interface number, which can be the number of any existing loopback interface. With this argument, this command displays information about a specified loopback interface.

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

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display interface loopback** to display information about a loopback interface.

- If you do not specify the **loopback** keyword, this command displays information about all interfaces on the device.
- If you specify the **loopback** keyword without the *interface-number* argument, this command displays information about all created loopback interfaces.

Related commands: **interface loopback**.

Examples

# Display detailed information about interface loopback 0.

```
<Sysname> display interface loopback 0
LoopBack0 current state: UP
Line protocol current state: UP (spoofing)
Description: LoopBack0 Interface
The Maximum Transmit Unit is 1536
Internet protocol processing : disabled
Physical is Loopback
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

# Display brief information about interface loopback 0.

```
<Sysname> display interface loopback 0 brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Loop0                UP   UP(s)    --
```

Table 12 Command output

Field	Description
current state	Physical state (up or administratively down) of the interface.

Field	Description
Line protocol current state	State of the data link layer protocol: up (spoofing). Spoofing refers to the spoofing attribute of the interface. When the network layer protocol state of the interface is displayed as up, the corresponding link may not exist, or the corresponding link is non-permanent and established on demand.
Description	Description string of the interface.
The Maximum Transmit Unit	Maximum transmission unit (MTU) of the interface.
Internet protocol processing	State (enabled or disabled) of the network layer protocol (displayed as **Internet Address is X.X.X.X/XX Primary**).
Physical is loopback	The physical type of the interface is loopback.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **reset counters interface** command. If the statistics of the interface have never been cleared by using the **reset counters interface** command since device startup, this field displays **Never**.
Last 300 seconds input: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic accounting), where the following conditions apply: • **packets/sec** indicates the average number of packets received per second. • **bytes/sec** indicates the average number of bytes received per second. • **bits/sec** indicates the average number of bits received per second.
Last 300 seconds output: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic accounting), where the following conditions apply: • **packets/sec** indicates the average number of packets sent per second. • **bytes/sec** indicates the average number of bytes sent per second. • **bits/sec** indicates the average number of bits sent per second.
0 packets input, 0 bytes, 0 drops	Total number and size (in bytes) of input packets of the interface and the number of dropped packets.
0 packets output, 0 bytes, 0 drops	Total number and size (in bytes) of output packets of the interface and the number of dropped packets.
The brief information of interface(s) under route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link status: • **ADM**—The interface has been administratively shut down. To recover its physical state, execute the **undo shutdown** command. • **Stby**—The interface is operating as a backup interface.

Field	Description
Protocol: (s) - spoofing	If the network layer protocol state of an interface is shown as UP, but its link is an on-demand link or not present at all, its protocol attribute includes the spoofing flag (an **s** in parentheses).
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The link is up. • **ADM**—The link has been administratively shut down. To recover its physical state, perform the **undo shutdown** command.
Protocol	Protocol connection state of the interface, which can be UP, DOWN, or UP(s).
Main IP	The main IP address of the interface.
Description	Description of the interface.
Cause	The cause of a DOWN physical link. If the port has been shut down with the **shutdown** command, this field displays **Administratively**. To restore the physical state of the interface, use the **undo shutdown** command.

NOTE:

The switch does not support collecting statistics about average input or output rate of loopback interfaces. These fields display **0**.

display interface null

Syntax

display interface [**null**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface null 0 [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

0: Specifies interface Null 0. The null interface number is fixed at 0, because the device has only one null interface.

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

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display interface null** to display information about the null interface. Because Null 0 interface is the only null interface on a device, this command displays information about Null 0 interface, even if you do not specify the **0** keyword.

- If you do not specify the **null** keyword, this command displays information about all interfaces on the device.
- If you specify the **null** keyword, this command displays information about interface Null 0 with or without the **0** keyword, because the device supports only one interface Null 0.

Related commands: **interface null**.

Examples

# Display detailed information about null interface Null 0.

```
<Sysname> display interface null 0
NULL0 current state :UP
Line protocol current state :UP (spoofing)
Description :  NULL0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

# Display brief information about interface Null 0.

```
<Sysname> display interface null 0 brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                UP   UP(s)    --
```

For the output description, seeTable 12.

NOTE:

The switch does not support collecting statistics about average input or output rate of interface Null 0. These fields display **0**.

interface loopback

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

View

System view

Default level

2: System level

Parameters

interface-number: Loopback interface number, ranging from 0 to 3.

Description

Use **interface loopback** to create a loopback interface or enter loopback interface view.

Use **undo interface loopback** to remove a loopback interface.

Related commands: **display interface loopback**.

Examples

# Create interface loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0]
```

interface null

Syntax

interface null 0

View

System view

Default level

2: System level

Parameters

0: Specifies interface Null 0. The null interface number is fixed to 0.

Description

Use **interface null** to enter null interface view.

A device has only one null interface, interface Null 0. Interface Null 0 is always up. You cannot remove or shut it down.

Related commands: **display interface null**.

Examples

# Enter Null 0 interface view.

```
<Sysname> system-view
[Sysname] interface null 0
[Sysname-NULL0]
```

reset counters interface loopback

Syntax

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

View

User view

Default level

2: System level

Parameters

interface-number: Number of the loopback interface, which can be the number of any existing loopback interface. With this argument, the command clears statistics on a specified loopback interface.

Description

Use **reset counters interface loopback** to clear statistics on loopback interfaces.

Before collecting traffic statistics within a specific period of time on a loopback interface, clear the existing statistics.

- If you do not specify the **loopback** keyword, this command clears the statistics on all interfaces in the system.
- If you specify the **loopback** keyword without the *interface-number* argument, this command clears the statistics on all loopback interfaces.

Examples

# Clear statistics on loopback interface Loopback 0.

```
<Sysname> reset counters interface loopback 0
```

reset counters interface null

Syntax

reset counters interface [**null** [**0**]]

View

User view

Default level

2: System level

Parameters

0: Number of the null interface, which is fixed at 0.

Description

Use **reset counters interface null** to clear statistics on the null interface.

Before collecting traffic statistics within a specific period of time on the null interface, clear the existing statistics.

- If you do not specify the **null** keyword, this command clears statistics on all interfaces.
- If you specify the **null** keyword, this command clears the statistics on interface Null 0 with or without the **0** keyword, because the device supports only one interface Null 0.

Examples

# Clear statistics on interface Null 0.

```
<Sysname> reset counters interface null 0
```

shutdown

Syntax

shutdown

undo shutdown

View

Loopback interface view

Default level

2: System level

Parameters

None

Description

Use **shutdown** to shut down the loopback interface.

Use **undo shutdown** to bring up the loopback interface.

By default, a loopback interface is up.

Examples

# Shut down loopback interface loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-Loopback0] shutdown
```

Bulk interface configuration commands

interface range

Syntax

interface range *interface-list*

View

System view

Default level

2: System level

Parameters

interface-list: Interface list in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>. The *interface-type interface-number* argument specifies an interface by its type and number. &<1-5> indicates that you can specify up to five interfaces or interface lists. When you specify the **to** keyword in *interface-type interface-number1* **to** *interface-type interface-number2*, the interfaces before and after the **to** keyword must be on the same interface card or subcard, and the interface number before **to** must be no greater than the one after **to**.

Description

Use **interface range** to create an interface range and enter interface range view.

You can use this command to enter interface range view to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, you can perform the **shutdown** command in interface range view to shut down a range of interfaces.

In interface range view, only the commands supported by the first interface are available. To view the commands supported by the first interface in the interface range, enter the interface range view and enter **?** at the command line interface prompt.

To verify the configuration of the first interface in the interface range, execute the **display this** command in interface range view.

Failure of applying a command on one member interface does not affect the application of the command on the other member interfaces. If applying a command on one member interface fails, the system displays an error message and continues with the next member interface.

Examples

# Shut down interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/24, VLAN interface 2,

```
<Sysname> system-view
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/24 vlan-interafce
2
[Sysname-if-range] shutdown
```

interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

Default level

2: System level

Parameters

name: Interface range name, a case-sensitive string of 1 to 32 characters.

interface-list: Interface list in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>. The *interface-type interface-number* argument specifies an interface by its type and number. &<1-5> indicates that you can specify up to five interfaces or interface lists. When you specify the **to** keyword in *interface-type interface-number1* **to** *interface-type interface-number2*, the interfaces before and after the **to** keyword must be on the same interface card or subcard, and the interface number before **to** must be no greater than the one after **to**.

Description

Use the **interface range name** *name* **interface** *interface-list* command to create an interface range, configure a name for the interface range, add interfaces to the interface range, and enter the interface range view.

Use the **interface range name** command without the **interface** keyword to enter the view of an interface range with the specified name.

Use **undo interface range name** to delete the interface range with the specified name.

You can use this command to assign a name to an interface range and can specify this name rather than the interface range to enter the interface range view.

You can use the **display current-configuration | include interface range** command to view the member interfaces of an interface range.

In interface range view, only the commands supported by the first interface are available. To view the commands supported by the first interface in the interface range, enter the interface range view and enter **?** at the command line interface prompt.

To verify the configuration of the first interface in the interface range, execute the **display this** command in interface range view.

Failure of applying a command on one member interface does not affect the application of the command on the other member interfaces. If applying a command on one member interface fails, the system displays an error message and continues with the next member interface.

When you bulk configure interfaces, follow these guidelines:

- Do not assign an aggregate interface and any of its member interfaces to an interface range at the same time. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- No limit is set on the maximum number of interfaces in an interface range. The more interfaces in an interface range, the longer the command execution time.

Examples

# Add GigabitEthernet 1/0/1 to GigabitEthernet 1/0/12 to interface range named **myEthPort**, and enter the interface range view.

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

```
[Sysname]   interface   range   name   myEthPort   interface   GigabitEthernet1/0/1   to
GigabitEthernet1/0/12
[Sysname-if-range-myEthPort]
```

# Enter the view of interface range named **myEthPort**.

```
<Sysname> system-view
[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]
```

MAC address table configuration commands

The MAC address table can contain only Layer 2 Ethernet ports and Layer 2 aggregate interfaces.

This feature covers only the unicast MAC address table. For information about configuring static multicast MAC address table entries for IGMP snooping and MLD snooping, see *IP Multicast Configuration Guide*.

display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

blackhole: Displays blackhole MAC address entries, which do not age and can be added and deleted. Packets with a matching source or destination MAC address are discarded.

vlan *vlan-id*: Displays MAC address entries of the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

count: Displays the number of MAC address entries specified by related parameters in the command. When this keyword is used, the command displays only the number of specified MAC address entries, rather than related information about these MAC address entries.

mac-address: Displays MAC address entries of a specified MAC address, in the format of H-H-H.

dynamic: Displays dynamic MAC address entries, which can be aged.

static: Displays static MAC address entries, which do not age.

interface *interface-type interface-number*: Displays the MAC address learning status of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-address** to display information about the MAC address table.

If you execute this command without specifying any parameters, it displays information of all MAC address entries on the device, including unicast MAC address entries and static multicast MAC address entries.

If you execute this command using only the **vlan** keyword or the **count** keyword, or only these two keywords, it displays information of unicast MAC address entries and static multicast MAC address entries.

Related commands: **mac-address (system view)**, **mac-address (interface view)**, and **mac-address timer**; **display mac-address multicast** and **display mac-address multicast count** (*IP Multicast Command Reference*).

Examples

# Display the MAC address table entry for MAC address 000f-e201-0101.

```
<Sysname> display mac-address 000f-e201-0101
MAC ADDR        VLAN ID    STATE            PORT INDEX              AGING TIME(s)
000f-e201-0101  1          Learned          GigabitEthernet1/0/1    AGING

  ---  1 mac address(es) found  ---
```

Table 13 Command output

Field	Description
MAC ADDR	MAC address.
VLAN ID	ID of the VLAN to which the MAC address belongs.
STATE	State of a MAC address entry: • **Config static**—The static entry manually configured by the user. • **Config dynamic**—The dynamic entry manually configured by the user. • **Learned**—The entry learned by the device. • **Blackhole**—The blackhole entry. • **Multicast**—The static multicast MAC address entry manually configured by the user. For more information about static multicast MAC address entries, see *IP Multicast Configuration Guide*.
PORT INDEX	Number of the port corresponding to the MAC address. Packets destined to this MAC address are sent out of this port. (Displayed as N/A for a blackhole MAC address entry).
AGING TIME(s)	Aging time: • **AGING**—The entry is aging. • **NOAGED**—The entry does not age.
1 mac address(es) found	One MAC address entry is found.

display mac-address aging-time

Syntax

display mac-address aging-time [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-address aging-time** to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (interface view)**, **mac-address timer**, and **display mac-address**.

Examples

# Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The output shows that the aging time of dynamic entries in the MAC address table is 300 seconds.

display mac-address mac-learning

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-address mac-learning** to display the MAC address learning status of the specified or all Layer 2 Ethernet ports.

Examples

# Display MAC address learning status of all Ethernet ports.

```
<Sysname> display mac-address mac-learning
Mac address learning status of the switch: enable

PortName                 Learning Status
GigabitEthernet1/0/1     enable
GigabitEthernet1/0/2     enable
GigabitEthernet1/0/3     enable
GigabitEthernet1/0/4     enable
```

Table 14 Command output

Field	Description
Mac-address learning status of the switch	Global MAC address learning status (enabled or disabled).
PortName	Port name.
Learning Status	MAC address learning status (enabled or disabled) for a port.

display mac-address statistics

Syntax

display mac-address statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-address statistics** to display the statistics of the MAC address table.

Examples

# Display the statistics of the MAC address table.

```
<Sysname> display mac-address statistics
MAC TYPE           LEARNED    USER-DEFINED  SYSTEM-DEFINED IN-USE    AVAILABLE
Dynamic   Unicast  26         0             1              27
Static    Unicast  0          1             2              3         1024
Total     Unicast                                          30        16384
```

```
Dynamic Multicast   0          0             0              0
Static  Multicast   0          0             2              2         512
Total   Multicast                                           2         512
```

Table 15 Command output

Field	Description
MAC TYPE	MAC address type: - Dynamic Unicast - Static Unicast - Total Unicast - Dynamic Multicast - Static Multicast - Total Multicast
LEARNED	Dynamically learned MAC addresses
USER-DEFINED	User defined MAC addresses (dynamic and static)
SYSTEM-DEFINED	MAC addresses generated by the system (for example, 802.1x and MAC authentication)
IN-USE	Number of existing MAC addresses of a specific type
AVAILABLE	Maximum number of MAC addresses supported by the system

mac-address (interface view)

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

dynamic: Specifies dynamic MAC address entries. These entries can age.

static: Specifies static MAC address entries. They do not age, but you can add or remove them.

mac-address: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted. For example, inputting "f-e2-1" indicates that the MAC address is "000f-00e2-0001".

vlan *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range of 1 to 4094.

Description

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

Use **undo mac-address** to remove a MAC address entry on the interface.

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

Related commands: **display mac-address**.

Examples

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

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

# Add a static entry for MAC address 000f-e201-0102 on port Bridge-Aggregation 1 that belongs to VLAN 1.

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

mac-address (system view)

Syntax

mac-address blackhole *mac-address* **vlan** *vlan-id*

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

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

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

View

System view

Default level

2: System level

Parameters

blackhole: Specifies blackhole MAC address entries. These entries do not age, but you can add or remove them. The packets whose source or destination MAC addresses match the blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted. For example, inputting "f-e2-1" indicates that the MAC address is "000f-00e2-0001".

vlan *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range of 1 to 4094.

dynamic: Specifies dynamic MAC address entries, which can be aged.

static: Specifies static MAC address entries. These entries do not age, but you can add or remove them.

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

Description

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

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

A static or blackhole MAC address entry will not be overwritten by a dynamic MAC address entry. A dynamic MAC address entry can be overwritten by a static or blackhole MAC address entry.

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 MAC address entries and static multicast MAC address entries) of a VLAN, or you can choose to delete a specific type (dynamic, static, or blackhole) of MAC address entries only. You can single out certain ports and delete the corresponding unicast MAC address entries, but not the corresponding static multicast MAC address entries.

The MAC address entries configuration cannot survive a reboot unless you save it. The dynamic MAC address table entries, however, are lost at next reboot regardless of whether or not you save the configuration.

Related commands: **display mac-address**.

Examples

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

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

mac-address mac-learning disable

Syntax

mac-address mac-learning disable

undo mac-address mac-learning disable

View

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

Default level

2: System level

Parameters

None

Description

Use **mac-address mac-learning disable** to disable MAC address learning. Depending on the view that you entered, you can disable it globally, on a Layer 2 interface, or a group of Ethernet ports.

Use **undo mac-address mac-learning disable** to enable MAC address learning. Depending on the view that you entered, you can disable it globally, on a Layer 2 interface, or a group of Ethernet ports.

By default, MAC address learning is enabled.

Follow these guidelines when you configure MAC address learning:

- You may need to disable MAC address learning to prevent the MAC address table from being saturated. For example, when your device is being attacked by many packets with different source MAC addresses, it affects the update of the MAC address table.
- Because disabling MAC address learning may result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on a port.

Related commands: **display mac-address mac-learning**.

NOTE:

When MAC address learning is disabled, the learned MAC addresses remain valid until they age out.

Examples

# Disable global MAC address learning.

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

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

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

# Disable MAC address learning on Bridge-Aggregation 1.

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

mac-address mac-roaming enable

Syntax

mac-address mac-roaming enable

undo mac-address mac-roaming enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **mac-address mac-roaming enable** to enable MAC address roaming.

Use **undo mac-address mac-roaming enable** to disable MAC address roaming.

By default, MAC address roaming is disabled.

Examples

# Enable MAC address roaming.

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

mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

count: Specifies the maximum number of MAC addresses that can be learned on a port. The value is in the range of 0 to 4096. When the argument takes 0, the VLAN is not allowed to learn MAC addresses.

Description

Use **mac-address max-mac-count** *count* to configure the maximum number of MAC addresses that can be learned on a port.

Use **undo mac-address max-mac-count** to restore the default maximum number of MAC addresses that can be learned on an Ethernet port.

By default, no MAC learning limit is configured.

If the command is executed in interface view, the configuration takes effect on the interface only. If the command is executed in port group view, the configuration takes effect on all ports in the port group.

Related commands: **mac-address** and **mac-address timer**.

Examples

# Set the maximum number of MAC addresses that can be learned on port GigabitEthernet 1/0/1 to 600.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

mac-address timer

Syntax

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

undo mac-address timer aging

View

System view

Default level

2: System level

Parameters

aging *seconds*: Sets an aging timer (in seconds) for dynamic MAC address entries. The value is in the range of 10 to 1,000,000 seconds.

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

Description

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

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

By default, the aging timer is 300 seconds.

Follow these guidelines to set the aging timer appropriately:

- A long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate the latest network changes.
- A short aging interval may result in removal of valid entries and unnecessary broadcasts that may affect the performance of the switch.

Examples

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

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

MAC Information configuration commands

MAC Information applies only to Layer 2 Ethernet interfaces.

mac-address information enable (Ethernet interface view)

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

View

Layer 2 Ethernet interface view

Default level

1: Monitor level

Parameters

added: Enables the device to record security information when a new MAC address is learned on the Ethernet port.

deleted: Enables the device to record security information when an existing MAC address is deleted.

Description

Use **mac-address information enable** to enable MAC Information on the Layer 2 Ethernet interface.

Use **undo mac-address information enable** to disable MAC Information on the Layer 2 Ethernet interface.

By default, MAC Information is disabled on a Layer 2 Ethernet interface.

This command is not supported on aggregate interfaces.

To enable MAC Information on an Ethernet interface, enable MAC Information globally.

Examples

# Enable MAC Information on GigabitEthernet 1/0/1.

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

mac-address information enable (system view)

Syntax

mac-address information enable

undo mac-address information enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **mac-address information enable** to enable MAC Information globally.

Use **undo mac-address information enable** to disable MAC Information globally.

By default, MAC Information is disabled globally.

Examples

# Enable MAC Information globally.

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

mac-address information interval

Syntax

mac-address information interval *value*

undo mac-address information interval

View

System view

Default level

2: System level

Parameters

value: Sets the interval for sending Syslog or trap messages, in the range of 1 to 20,000 seconds.

Description

Use **mac-address information interval** to set the interval for sending Syslog or trap messages.

Use **undo mac-address information interval** to restore the default interval for sending Syslog or trap messages.

By default, the interval for sending Syslog or trap messages is 1 second.

Examples

# Set the interval for sending Syslog or trap messages to 200 seconds.

```
<Sysname> system-view
[Sysname] mac-address information interval 200
```

mac-address information mode

Syntax

mac-address information mode { **syslog** | **trap** }

undo mac-address information mode { **syslog** | **trap** }

View

System view

Default level

2: System level

Parameters

syslog: Specifies that the device sends Syslog messages to inform the remote network management device of MAC address changes.

trap: Specifies that the device sends trap messages to inform the remote network management device of MAC address changes.

Description

Use **mac-address information mode** to set the MAC Information mode (to use Syslog messages or trap messages) to inform the remote network management device of MAC address changes.

Use **undo mac-address information mode** to restore the default.

By default, trap messages are sent to inform the remote network management device of MAC address changes.

Examples

# Configure the device to send trap messages to inform the remote network management device of MAC address changes.

```
<Sysname> system-view
[Sysname] mac-address information mode trap
```

mac-address information queue-length

Syntax

mac-address information queue-length *value*

undo mac-address information queue-length

View

System view

Default level

2: System level

Parameters

value: Specifies the MAC Information queue length, in the range of 0 to 1000.

Description

Use **mac-address information queue-length** to set the MAC Information queue length.

Use **undo mac-address information queue-length** to restore the default.

By default, the MAC Information queue length is 50.

When you set the MAC Information queue length to 0, it indicates that the device will send a Syslog or trap message to the network management device as soon as a new MAC address is learned or an existing MAC address is deleted.

Examples

# Set the MAC Information queue length to 600.

```
<Sysname> system-view
[Sysname] mac-address information queue-length 600
```

Ethernet link aggregation configuration commands

default

Syntax

default

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

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

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

△ CAUTION:

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

Examples

# Restore the default settings for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Syntax

description *text*

undo description

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

text: Specifies the interface description, a string of 1 to 80 characters.

Description

Use **description** to set a description for an interface. Fore example, you can include information such as the purpose of the interface for the ease of management.

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

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

Examples

# Set the description of Layer 2 aggregate interface Bridge-Aggregation 1 to **connect to the lab**.

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

display interface

Syntax

display interface [**bridge-aggregation**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

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

View

Any view

Default level

1: Monitor level

Parameters

bridge-aggregation: Displays information about Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number. The value range for the *interface-number* argument is the set of all existing aggregate interface numbers.

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

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

If **bridge-aggregation** is not specified, this command displays information about all interfaces.

If **bridge-aggregation** is specified without any interface number specified, this command displays information about all aggregate interfaces.

If **bridge-aggregation** *interface-number* is specified, this command displays information about the specified aggregate interface.

Examples

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

```
<Sysname> display interface bridge-aggregation 1
 Bridge-Aggregation1 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e207-f2e0
 Description: Bridge-Aggregation1 Interface
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 PVID: 1
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Last clearing of counters:  Never
 Last 300 seconds input:  0 packets/sec 0 bytes/sec    -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec    -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
```

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

```
<Sysname> display interface bridge-aggregation 1 brief
The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                DOWN auto    A      A    1
```

Table 16 Command output

Field	Description
Bridge-Aggregation1 current state	The Layer 2 interface status: • **DOWN (Administratively)**—The interface is administratively shut down with the **shutdown** command. • **DOWN**—The interface is administratively up but physically down (possibly because no physical link is present or the link is faulty). • **UP**—The Ethernet interface is both administratively and physically up.
Unknown-speed mode, unknown-duplex mode	The interface speed and duplex mode are unknown.
PVID	The port VLAN ID (PVID).
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. **Never** indicates the **reset counters interface** command has never been used on the interface since the device's startup.
Last 300 seconds input/output	The average input/output rate over the last 300 seconds.
Input/Output (total)	The statistics of all packets received/sent on the interface.
Input/Output (normal)	The statistics of all normal packets received/sent on the interface.
The brief information of interface(s) under bridge mode	Brief information about Layer 2 interfaces.
Link: ADM - administratively down; Stby - standby	Link status: • **ADM**—The interface has been administratively shut down. To recover its physical layer state, perform the **undo shutdown** command. • **Stby**—The interface is operating as a backup interface.
Speed or Duplex: (a)/A - auto; H - half; F - full	If the speed of an interface is automatically negotiated, its speed attribute includes the auto negotiation flag, letter **a** in parentheses. If the duplex mode of an interface is automatically negotiated, its duplex mode attribute includes the auto negotiation flag, letter **a** in parentheses or a capital **A**. Letter **H** indicates the half duplex mode, and letter **F** indicates the full duplex mode.
Type: A - access; T - trunk; H - hybrid	Link type options for Ethernet interfaces.
Interface	The abbreviated interface name.
Link	The physical link state of the interface.
Speed	The interface speed, in bps.

display lacp system-id

Syntax

display lacp system-id [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

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

Use **lacp system-priority** to change the LACP priority of the local system. Although you specify the LACP priority value in decimal format in the **lacp system-priority** command, it is displayed as a hexadecimal value with the **display lacp system-id** command.

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

Examples

# Display the local system ID.

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

Table 17 Command output

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

display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

interface-number: Specifies an existing aggregate interface number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

To display the global link-aggregation load sharing criteria, run the command without the **interface** keyword.

To display all the group-specific load sharing criteria, run the command with the **interface** keyword, but do not specify a particular interface.

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

The **bridge-aggregation** keyword becomes available only after you create Layer 2 aggregate interfaces on the device.

Examples

# Display the global link-aggregation load sharing criteria.

```
<Sysname>display link-aggregation load-sharing mode
Link-Aggregation Load-Sharing Mode:
Layer 2 traffic: ingress-port,           destination-mac address,
                 source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

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

```
<Sysname>display link-aggregation load-sharing mode interface Bridge-Aggregation 10
Bridge-Aggregation10 Load-Sharing Mode:
Layer 2 traffic: ingress-port,           destination-mac address,
                 source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Table 18 Command output

Field	Description
Link-Aggregation Load-Sharing Mode	The global link-aggregation load sharing criteria.
Bridge-Aggregation10 Load-Sharing Mode	Link-aggregation load sharing criteria of the aggregation group corresponding to the aggregate interface Bridge-Aggregation 10.
Layer 2 traffic: ingress-port, destination-mac address, source-mac address	The default link-aggregation load sharing criteria for Layer 2 traffic. In this sample output, the criteria are the ingress-port, the source MAC address, and the destination MAC addresses of packets.

Field	Description
Layer 3 traffic: destination-ip address, source-ip address	The default link-aggregation load sharing criteria for Layer 3 traffic. In this sample output, the criteria are the source and destination IP addresses of packets.

display link-aggregation member-port

Syntax

display link-aggregation member-port [*interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* indicates the port type and port number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display link-aggregation member-port** to display detailed link aggregation information for the specified member ports. If no port is specified, this command displays detailed link aggregation information for all member ports.

Only the port number and operational key of a member port in a static aggregation group are displayed, because the aggregation group is not aware of the partner's information.

Examples

# Display detailed link aggregation information for GigabitEthernet 1/0/1, 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:
Aggregation Interface: Bridge-Aggregation1
Port Number: 3
Port Priority: 32768
```

```
Oper-Key: 2
```

# Display detailed link aggregation information for GigabitEthernet 1/0/2, 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:
Aggregation Interface: Bridge-Aggregation2
Local:
    Port Number: 7
    Port Priority: 32768
    Oper-Key: 3
    Flag: {ACG}
Remote:
    System ID: 0x8000, 0000-0000-0000
    Port Number: 0
    Port Priority: 32768
    Oper-Key: 0
    Flag: {EF}
Received LACP Packets: 0 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 0 packet(s)
```

Table 19 Command output

Field	Description
Flags	LACP state flags: • **A**—LACP is enabled. • **B**—Indicates the LACP short timeout. • **C**—The sending system detects that the link is aggregatable. • **D**—The sending system detects that the link is synchronized. • **E**—The sending system detects that the incoming frames are collected. • **F**—The sending system detects that the outgoing frames are distributed. • **G**—The sending system receives frames in the default state. • **H**—The sending system receives frames in the expired state.
Aggregation Interface	Aggregate interface to which the member port belongs.
Local	Information about the local end.
Port Priority	Aggregation priority of the port.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the remote end.
System ID	The remote end system ID, comprising the system LACP priority and the system MAC address.
Received LACP Packets	Total number of LACP packets received.

Field	Description
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

display link-aggregation summary

Syntax

display link-aggregation summary [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

The information about the remote system for a static link aggregation group may be displayed as **none** or may not be displayed, because the aggregation group is not aware of the partner's information.

Examples

# Display the summary information for all aggregation groups.

```
<Sysname> display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

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

Table 20 Command output

Field	Description
Aggregation Interface Type	Aggregate interface type: • **BAGG**—Layer 2 aggregate interface. • **RAGG**—Layer 3 aggregate interface.
Aggregation Mode	Aggregation group type: • **S**—Static link aggregation. • **D**—Dynamic aggregation.
Loadsharing Type	Load sharing type: • **Shar**—Load sharing. • **NonS**—Non-load sharing.
Actor System ID	Local system ID, which comprises the system LACP priority and the system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the partner, which comprises the system LACP priority and the system MAC address.
Select Ports	Total number of Selected ports.
Unselect Ports	Total number of Unselected ports.
Share Type	Load sharing type.

display link-aggregation verbose

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

interface-number: Specifies an existing aggregate interface number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Use **display link-aggregation verbose bridge-aggregation** *interface-number* to display information about a specific Layer 2 aggregation group.

Use **display link-aggregation verbose bridge-aggregation** to display information about all Layer 2 aggregation groups,.

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

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

Examples

# Display detailed information about the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 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
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
-------------------------------------------------------------------------------
  GE1/0/26           S       32768    2         {ACDEF}
  GE1/0/32           S       32768    2         {ACDEF}
Remote:
  Actor           Partner Priority Oper-Key  SystemID               Flag
-------------------------------------------------------------------------------
  GE1/0/26           32      32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/32           26      32768    2         0x8000, 000f-e267-57ad {ACDEF}
```

# Display detailed information about the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 2, which is a static aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: NonS
```

```
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  GE1/0/21           U       32768     1
  GE1/0/22           U       32768     1
  GE1/0/23           U       63        1
```

Table 21 Command output

Field	Description
Loadsharing Type	Load sharing type: • Shar—Load sharing. • NonS—Non-load sharing.
Port Status	Port state: Selected or unselected.
Flags	LACP state flags: • **A**—LACP is enabled. • **B**—Indicates the LACP short timeout. • **C**—The sending system detects that the link is aggregatable. • **D**—The sending system detects that the link is synchronized. • **E**—The sending system detects that the incoming frames are collected. • **F**—The sending system detects that the outgoing frames are distributed. • **G**—The sending system receives frames in the default state. • **H**—The sending system receives frames in the expired state.
Aggregation Interface	Name of the aggregate interface.
Aggregation Mode	Mode of the aggregation group: • Static for static aggregation. • Dynamic for dynamic aggregation.
System ID	Local system ID, comprising the system LACP priority and the system MAC address.
Local	Information about the local end.
Port	Port type and number.
Status	Port state: selected or unselected.
Priority	Port aggregation priority.
Oper-Key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the remote end.
Actor	Local port type and number.
Partner	Remote port index.

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

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

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

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

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

For more information about the **snmp-agent trap enable** command, see *Network Management and Monitoring Command Reference*.

Examples

# Enable linkUp/linkDown trap generation on Layer 2 aggregate interface Bridge-Aggregation 1.

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

interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

View

System view

Default level

2: System level

Parameters

interface-number: Specifies a Layer 2 aggregate interface by its number, in the range of 1 to 128.

Description

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

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

When you create a Layer 2 aggregate interface, a Layer 2 aggregation group with the same number is automatically created. If you remove the Layer 2 aggregate interface, you also remove the Layer 2 aggregation group, and any member ports will 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]
```

lacp period short

Syntax

lacp period short

undo lacp period

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **lacp period short** to set the LACP timeout interval on a port to the short timeout interval (1 second).

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

The default LACP timeout interval is the long timeout interval (30 seconds).

Examples

# Set the LACP timeout interval on GigabitEthernet 1/0/1 to the short timeout interval (1 second).

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

lacp system-priority

Syntax

lacp system-priority *system-priority*

undo lacp system-priority

View

System view

Default level

2: System level

Parameters

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

Description

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

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

By default, the system LACP priority is 32768.

Examples

# Set the system LACP priority to 64.

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

link-aggregation lacp traffic-redirect-notification enable

Syntax

link-aggregation lacp traffic-redirect-notification enable

undo link-aggregation lacp traffic-redirect-notification enable

View

System view

Default level

2: System level

Parameters

None

Description

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.

By default, link-aggregation traffic redirection is disabled.

Link-aggregation traffic redirection 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.

Do not enable both MSTP and link-aggregation traffic redirection at the same time, because light packet loss may occur when the device reboots.

After link-aggregation traffic redirection is enabled, do not add an Ethernet interface configured with physical state change suppression to an aggregation group. Otherwise, Selected ports in the aggregation group might work improperly. For more information about physical state change suppression, see the **link-delay** command in "Ethernet interface configuration commands."

Examples

# Enable link-aggregation traffic redirection.

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

link-aggregation load-sharing mode

Syntax

In system view:

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

undo link-aggregation load-sharing mode

In Layer 2 aggregate interface view:

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

undo link-aggregation load-sharing mode

View

System view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

destination-ip: Performs load sharing in link aggregation groups based on destination IP address.

destination-mac: Performs load sharing in link aggregation groups based on destination MAC address.

destination-port: Performs load sharing in link aggregation groups based on destination port.

ingress-port: Performs load sharing in link aggregation groups based on ingress port.

source-ip: Performs load sharing in link aggregation groups based on source IP address.

source-mac: Performs load sharing in link aggregation groups based on source MAC address.

source-port: Performs load sharing in link aggregation groups based on source port.

Description

Use **link-aggregation load-sharing mode** to configure the global or group-specific link-aggregation load sharing criteria.

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

By default, the system selects the load sharing criteria according to the packet type, and the group-specific link-aggregation load sharing criteria are the same as the global ink-aggregation load sharing criteria.

This command applies to only unicast packets, and can change the load sharing criteria for unicast packets. Broadcast packets and multicast packets always use the default load sharing criteria.

The load sharing criteria that you configure will overwrite the previous criteria.

If unsupported load sharing criteria are configured, an error prompt will appear.

In system view, the switch supports the following load sharing criteria and combinations:

- Source IP address
- Destination IP address

- Source MAC address
- Destination MAC address
- Source IP address and destination IP address
- Source IP address and source port
- Destination IP address and destination port
- Any combination of incoming port, source MAC address, and destination MAC address

In Layer 2 aggregate interface view, the switch supports the following load sharing criteria and combinations:

- Automatic load sharing criteria determined based on the packet type
- Source IP address
- Destination IP address
- Source MAC address
- Destination MAC address
- Destination IP address and source IP address
- Destination MAC address and source MAC address

Examples

# Configure the destination MAC address as the global link-aggregation load sharing criterion.

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

# Configure the destination MAC address as the load sharing criterion specific to the link aggregation group of aggregate interface Bridge-Aggregation 1.

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

link-aggregation load-sharing mode local-first

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

View

System view

Default level

2: System level

Parameters

None

Description

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.

By default, local-first load sharing is enabled for link aggregation.

Examples

# Disable local-first load sharing for link aggregation.

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

link-aggregation mode

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

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

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

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

To change the aggregation mode of an aggregation group that contains member ports, remove all the member ports from the aggregation group first.

Examples

# Configure the aggregation group corresponding to Bridge-Aggregation 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

Syntax

link-aggregation port-priority *port-priority*

undo link-aggregation port-priority

View

Ethernet interface view

Default level

2: System level

Parameters

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

Description

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

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

The default aggregation priority of a port is 32768.

Examples

# Set the aggregation priority of port GigabitEthernet 1/0/1 to 64.

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

link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *number*

undo link-aggregation selected-port maximum

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of Selected ports allowed in an aggregation group. This argument ranges from 1 to 8.

Description

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

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

By default, the maximum number of Selected ports allowed in an aggregation group is limited only by the hardware capabilities of the member ports.

Executing this command may cause some of the member ports in the aggregation group to become unselected.

The maximum numbers of Selected ports for the local and peer aggregation groups must be consistent.

Examples

# Configure the maximum number of Selected ports as 3 in the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 1.

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

link-aggregation selected-port minimum

Syntax

link-aggregation selected-port minimum *number*

undo link-aggregation selected-port minimum

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface. This argument ranges from 1 to 8.

Description

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

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

By default, the minimum number of Selected ports in an aggregation group is not specified.

Executing this command may cause all the member ports in the aggregation group to become unselected.

The minimum numbers of Selected ports for the local and peer aggregation groups must be consistent.

Examples

# Configure the minimum number of Selected ports as 3 in the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 1.

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

port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

View

Ethernet interface view

Default level

2: System level

Parameters

number: Specifies the number of the aggregate interface corresponding to an aggregation group. The *number* argument ranges from 1 to 128.

Description

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

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

An Ethernet 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

Syntax

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

View

User view

Default level

2: System level

Parameters

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

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

Description

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

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

- If no keywords or argument is specified, the command clears the statistics of all interfaces in the system.
- If only the **bridge-aggregation** keyword is specified, the command clears the statistics of all Layer 2 aggregate interfaces.
- If the **bridge-aggregation** *interface-number* keyword and argument combination is specified, the command clears the statistics of the specified Layer 2 aggregate interface.
- The **bridge-aggregation** keyword becomes available only after you create Layer 2 aggregate interfaces on the device.

Examples

# Clear the statistics of Layer 2 aggregate interface Bridge-Aggregation 1.

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

reset lacp statistics

Syntax

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

View

User view

Default level

1: Monitor level

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* indicates the port type and port number.

Description

Use **reset lacp statistics** to clear the LACP statistics on the specified member ports or all member ports, if no member ports are specified.

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

Examples

# Clear the LACP statistics on all link aggregation member ports.

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

shutdown

Syntax

shutdown

undo shutdown

View

Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **shutdown** to shut down the aggregate interface.

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

By default, aggregate interfaces are up.

Examples

# Shut down Layer 2 aggregate interface Bridge-Aggregation 1.

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

Port isolation configuration commands

display port-isolate group

Syntax

display port-isolate group [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

# Display port isolation group information.

```
<Sysname> display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
 Group members:
    GigabitEthernet1/0/2
```

Table 22 Command output

Field	Description
Port-isolate group information	Display port isolation group information.
Uplink port support	The switch series does not support configuring an uplink port in the port isolation group.
Group ID	Isolation group number. It can only be 1.
Group members	Isolated ports in the isolation group.

port-isolate enable

Syntax

port-isolate enable

undo port-isolate enable

View

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

Default level

2: System level

Parameters

None

Description

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

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

- To assign Ethernet ports to the isolation group one by one, perform the command in Ethernet interface view.
- To bulk assign Ethernet ports to the isolation group, perform the command in port group view.
- To assign a Layer 2 aggregate interface to the isolation group, perform the command in Layer 2 aggregate interface view. The configuration applies to the Layer 2 aggregate interface and all its member ports. If the switch fails to apply the **port-isolate enable** command to a Layer 2 aggregate interface, it does not assign any member port of the aggregate interface to the isolation group. If the failure occurs on a member port, the switch can still assign other member ports to the isolation group. For more information about Layer 2 aggregate interfaces, see *Layer 2—LAN Switching Configuration Guide*.

Examples

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

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

# Assign all ports in port group **aa** to the isolation group.

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

# Assign Layer 2 aggregate interface Bridge-Aggregation 1 to the 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
```

Spanning tree configuration commands

active region-configuration

Syntax

active region-configuration

View

MST region view

Default level

2: System level

Parameters

None

Description

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

When you configure MST region–related parameters, MSTP launches a new spanning tree calculation process that may cause network topology instability. This is mostly likely to occur when you configure the VLAN-to-instance mapping table. The launch will only occur after you activate the MST region–related parameters by using **active region-configuration** command or enable MSTP by using the **stp enable** command.

HP recommends that you 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.

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

Examples

# Map VLAN 2 to MSTI 1 and manually 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
```

bpdu-drop any

Syntax

bpdu-drop any

undo bpdu-drop any

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **bpdu-drop any** to enable BPDU drop on a port.

Use **undo bpdu-drop any** to disable BPDU drop on a port.

By default, BPDU drop is disabled on a port.

Examples

# Enable BPDU drop on port GigabitEthernet 1/0/1.

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

check region-configuration

Syntax

check region-configuration

View

MST region view

Default level

2: System level

Parameters

None

Description

Use **check region-configuration** to display MST region pre-configuration information, including the region name, revision level, and VLAN-to-instance mapping settings.

Two or more spanning tree devices belong to the same MST region only if they are configured with the same format selector (0 by default, not configurable), MST region name, MST region revision level, and the same VLAN-to-instance mapping entries in the MST region, and if they are connected via a physical link.

HP recommends that you use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

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

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          :000fe26a58ed
   Revision level       :0
```

```
Configuration digest :0x41b5018aca57daa8dcfdba2984d99d06

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

Table 23 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.

display stp

Syntax

display stp [**instance** *instance-id* | **vlan** *vlan-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

instance *instance-id*: Displays the status and statistics of a specific MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the common internal spanning tree (CIST).

vlan *vlan-id*: Displays the spanning tree status and statistics of a VLAN specified by *vlan-id*, in the range of 1 to 4094.

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

slot *slot-number*: Displays the MSTP status and statistics on the specified IRF member switch. *slot-number* represents the member number of the device in the IRF. If this keyword-argument combination is not specified, this command displays the MSTP status and statistics on all IRF member switches.

brief: Displays brief spanning tree status and statistics.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stp** to display the spanning tree status and statistics.

Based on the spanning tree status and statistics, you can analyze and maintain the network topology or check whether spanning tree is working properly.

In STP/RSTP mode, follow these guidelines:

- If you do not specify any port, this command displays the spanning tree information for all ports. The displayed information is sorted by port name.
- If you specify a port list, this command displays the spanning tree information for the specified ports. The displayed information is sorted by port name.

In MSTP mode, follow these guidelines:

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

In PVST mode, follow these guidelines:

- If you do not specify any VLAN or port, this command displays the spanning tree information of all VLANs on all ports. The displayed information is sorted by VLAN ID and by port name in each VLAN.
- If you specify a VLAN but not a port, this command displays the spanning tree information on all ports in that VLAN. The displayed information is sorted by port name.
- If you specify some ports but not any VLAN, this command displays the spanning tree information of all VLANs on the specified ports. The displayed information is sorted by VLAN ID, and by port name in each VLAN.
- If you specify both a VLAN ID and a port list, this command displays the spanning tree information on the specified ports in the specified VLAN. The displayed information is sorted by port name.

The MSTP status information includes the following parameters:

- CIST global parameters:
    - Protocol operating mode
    - Device priority in the CIST (Priority)
    - MAC address
    - Hello time
    - Max age
    - Forward delay
    - Maximum hops
    - Common root bridge of the CIST
    - External path cost from the device to the CIST common root
    - Regional root

    - Internal path cost from the device to the regional root
    - CIST root port of the device
    - Status of the BPDU guard function (enabled or disabled)
- CIST port parameters:
    - Port status
    - Role
    - Priority
    - Path cost
    - Designated bridge
    - Designated port
    - Edge port/non-edge port
    - Connecting to a point-to-point link or not
    - Maximum transmission rate (transmit limit)
    - Status of the root guard function (enabled or disabled)
    - BPDU format
    - Boundary port/non-boundary port
    - Hello time
    - Max age
    - Forward delay
    - Message age
    - Remaining hops
    - Status of rapid state transition (enabled or disabled) for designated ports
- MSTI global parameters:
    - MSTI ID
    - Bridge priority of the MSTI
    - Regional root
    - Internal path cost
    - MSTI root port
    - Master bridge
- MSTI port parameters:
    - Port status
    - Role
    - Priority
    - Path cost
    - Designated bridge
    - Designated port
    - Remaining hops
    - Status of rapid state transition (enabled or disabled) for designated ports

The PVST status information includes the following parameters:

- Global parameters:
    - Device priority in the VLAN
    - MAC address
    - Hello time
    - Max age
    - Forward delay
    - Root bridge
    - Path cost from the device to the root bridge
    - Root port
    - Status of the BPDU guard function (enabled or disabled)
    - Number of received TC/TN BPDUs
    - Time since the last topology change
- Port parameters:
    - Port status
    - Role
    - Priority
    - Path cost
    - Designated bridge
    - Designated port
    - Edge port/non-edge port
    - Connecting to a point-to-point link or not
    - Maximum transmission rate (transmit limit)
    - Status of the root guard function (enabled or disabled)
    - Hello time
    - Max age
    - Forward delay
    - Message age
    - Status of rapid state transition (enabled or disabled) for designated ports

The statistics in STP/RSTP/MSTP mode include the following items:

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

Related commands: **reset stp**.

Examples

# In MSTP mode, display the brief spanning tree status and statistics of MSTI 0 on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
brief
 MSTID      Port                             Role  STP State     Protection
```

```
   0       GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
   0       GigabitEthernet1/0/2         DESI  FORWARDING    NONE
   0       GigabitEthernet1/0/3         DESI  FORWARDING    NONE
   0       GigabitEthernet1/0/4         DESI  FORWARDING    NONE
```

# In PVST mode, display the brief spanning tree status and statistics of VLAN 2 on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4 brief
 VLAN      Port                         Role  STP State     Protection
    2      GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
    2      GigabitEthernet1/0/2         DESI  FORWARDING    NONE
    2      GigabitEthernet1/0/3         DESI  FORWARDING    NONE
    2      GigabitEthernet1/0/4         DESI  FORWARDING    NONE
```

Table 24 Command output

Field	Description
MSTID	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	Protection type on the port: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. • **BPDU/ROOT**—BPDU guard and root guard. • **NONE**—No protection.

# In MSTP mode, display the spanning tree status and statistics of all MSTIs on all ports.

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

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

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

# In PVST mode, display the spanning tree status and statistics of all VLANs on all ports.

```
<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 FwDly 15s
Root ID / RPC       :0.00e0-fc0e-6554 / 200200
Root PortId         :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 Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :32768.000f-e200-2200 / 128.2
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :false
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s
 BPDU Sent           :186
          TCN: 0, Config: 0, RST: 0
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0

-------[VLAN 2 Global Info]-------
Protocol Status     :enabled
Bridge ID           :32768.000f-e200-2200
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :0.00e0-fc0e-6554 / 200200
Root PortId         :128.48
BPDU-Protection     :disabled
TC or TCN received  :2
Time since last TC  :0 days 0h:5m:42s
```

# 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
```

Table 25 Command output

Field	Description
CIST Bridge	CIST bridge ID, which comprises the device's priority in the CIST and its MAC address. For example, in output "32768.000f-e200-2200", the value preceding the dot is the device's priority in the CIST, and the value following the dot is the device's MAC address.

Field	Description
Bridge ID	Bridge ID, which comprises the device's priority in VLAN 1 and its MAC address. For example, in output "32768.000f-e200-2200", the value preceding the dot is the device's priority in VLAN 1, and the value following the dot is the device's MAC address.
Bridge Times	Major parameters for the bridge: • **Hello**—Hello timer. • **MaxAge**—Max age timer. • **FWDly**—Forward delay timer. • **Max Hop**—Max hops within the MST region.
CIST Root/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
CIST RegRoot/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the CIST regional root).
Root ID / RPC	VLAN root ID and root path cost (the path cost from the device to the root).
CIST RootPortId	CIST root port ID. "0.0" indicates that the device is the root and there is no root port.
Root PortId	VLAN root port ID. "0.0" indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of BPDU protection.
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.
[FORWARDING]	The port is in forwarding state.
[DISCARDING]	The port is in discarding state.
[LEARNING]	The port is in learning state.
Port Protocol	Status of the spanning tree feature on the port.
Port Role	Port role, which can be Alternate, Backup, Root, Designated, Master, or Disabled.
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.

Field	Description
Transmit Limit	Maximum number of packets sent within each hello time.
Protection Type	Protection type on the port: • **Root**—Root guard. • **Loop**—Loop guard. • **BPDU**—BPDU guard. • **BPDU/ROOT**—BPDU guard and root guard. • **None**—No protection.
MST BPDU Format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s. • **Config**—Configured value. • **Active**—Actual value.
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	The port rapidly transitions to the forwarding state or not in the MSTI or VLAN.
Num of Vlans Mapped	Number of VLANs mapped to the MSTI.
PortTimes	Major parameters for the port: • **Hello**—Hello timer. • **MaxAge**—Max Age timer. • **FWDly**—Forward delay timer. • **MsgAge**—Message Age timer. • **Remain Hop**—Remaining hops.
BPDU Sent	Statistics on sent BPDUs.
BPDU Received	Statistics on received BPDUs.
MSTI RegRoot/IRPC	MSTI regional root/internal path cost.
MSTI RootPortId	MSTI root port ID.
MSTI Root Type	MSTI root type, which can be **primary root** or **secondary root**.
Master Bridge	MSTI root bridge ID.
Cost to Master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.
Protocol Status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	In MSTP mode, this field indicates the device's priority in the CIST. In PVST mode, this field indicates the device's priority in VLAN 1.
Max age(s)	Aging timer (in seconds) for BPDUs. In PVST mode, this field is the configuration in VLAN 1.
Forward delay(s)	Port state transition delay (in seconds). In PVST mode, this field is the configuration in VLAN 1.
Hello time(s)	Interval (in seconds) for the root bridge to send BPDUs. In PVST mode, this field is the configuration in VLAN 1.
Max hops	Maximum hops in the MSTI.

display stp abnormal-port

Syntax

display stp abnormal-port [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stp abnormal-port** to display information about ports blocked by spanning tree protection functions.

Examples

# In MSTP mode, display information about ports blocked by spanning tree protection functions.

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

# In PVST mode, display information about ports blocked by spanning tree protection functions.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
 VLAN      Blocked Port                 Reason
    1      GigabitEthernet1/0/1         ROOT-Protected
    2      GigabitEthernet1/0/2         LOOP-Protected
    2      GigabitEthernet1/0/3         Formatcompatibility–Protected
```

Table 26 Command output

Field	Description
Blocked Port	Name of a blocked port, which corresponds to the related MSTI or VLAN.

Field	Description
Reason	Reason that the port was blocked: • **ROOT-Protected**—Root guard function. • **LOOP-Protected**—Loop guard function. • **Formatcompatibility-Protected**—MSTP BPDU format incompatibility protection function. • **InconsistentPortType-Protected**—Port type inconsistent protection function. • **InconsistentPvid-Protected**—PVID inconsistent protection function.

display stp bpdu-statistics

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the BPDU statistics on a specified port, where *interface-type interface-number* indicates the port type and number.

instance *instance-id*: Displays the BPDU statistics of a specified MSTI on a specified port. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stp bpdu-statistics** to display the BPDU statistics on ports.

In MSTP mode, follow these guidelines:

- If you do not specify any MSTI or port, this command displays the BPDU statistics of all MSTIs on all ports. The displayed information is sorted by port name and by MSTI ID on each port.
- If you specify a port but not an MSTI, this command displays the BPDU statistics of all MSTIs on the port. The displayed information is sorted by MSTI ID.
- If you specify both an MSTI ID and a port, this command displays the BPDU statistics of the specified MSTI on the port.

In STP, RSTP, or PVST mode, follow these guidelines:

- If you do not specify any port, this command displays the BPDU statistics of on all ports. The displayed information is sorted by port name.

- If you specify a port, this command displays the BPDU statistics on the port.

Examples

# In MSTP mode, display the BPDU statistics of 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 01/13/2010
 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

 Instance 0:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 MAX-hoped BPDUs             0
 TC detected                 1          10:32:40 01/13/2010
 TC sent                     3          10:33:11 01/13/2010
 TC received                 0

 Instance 1:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 MAX-hoped BPDUs             0
 TC detected                 0
 TC sent                     0
 TC received                 0

 Instance 2:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 MAX-hoped BPDUs             0
 TC detected                 0
 TC sent                     0
 TC received                 0
```

# In PVST mode, display the BPDU statistics on 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
```

Table 27 Command output

Field	Description
Port	Port name.
Instance-independent	Statistics not related to any particular MSTI.
Type	Statistical item.
Looped-back BPDUs	BPDUs sent and then received by the same port.
Max-Aged BPDUs	BPDUs whose max age was exceeded.
TCN Sent	TCN BPDUs sent.
TCN Received	TCN BPDUs received.
TCA Sent	TCA BPDUs sent.
TCA Received	TCA BPDUs received.
Config Sent	Configuration BPDUs sent.

Field	Description
Config Received	Configuration BPDUs received.
RST Sent	RSTP BPDUs sent.
RST Received	RSTP BPDUs received.
MST Sent	MSTP BPDUs sent.
MST Received	MSTP BPDUs received.
Instance	Statistical information for a particular MSTI.
Timeout BPDUs	Expired BPDUs.
Max-Hoped BPDUs	BPDUs whose maximum hops were exceeded.
TC Detected	TC BPDUs detected.
TC Sent	TC BPDUs sent.
TC Received	TC BPDUs received.

display stp down-port

Syntax

display stp down-port [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stp down-port** to display information about ports shut down by spanning tree protection functions.

Examples

# Display information about ports shut down by spanning tree protection functions.

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

Table 28 Command output

Field	Description
Down Port	Name of a port shut down by the spanning tree protection functions.
Reason	Reason that the port was shut down: • **BPDU-Protected**—BPDU guard function. • **Formatfrequency-Protected**—MSTP BPDU format frequent change protection function.

display stp history

Syntax

display stp [**instance** *instance-id* | **vlan** *vlan-id*] **history** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

0: Visit level

Parameters

instance *instance-id*: Displays the historical port role calculation information of a specific MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

vlan *vlan-id*: Displays the historical port role calculation information for a specific VLAN, in the range of 1 to 4094.

slot *slot-number*: Displays the historical port role calculation information on the specified IRF member switch. *slot-number* represents the number of the member number of the device in the IRF. If this keyword-argument combination is not specified, this command displays the historical port role calculation information on all IRF member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

In STP/RSTP mode, the displayed information is sorted by port role calculation time.

In MSTP mode, follow these guidelines:

- If you do not specify any MSTI, this command displays the historical port role calculation information of all MSTIs. The displayed information is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you specify an MSTI, this command displays the historical port role calculation information of the specified MSTI by the sequence of port role calculation time.

In PVST mode, follow these guidelines:

- If you do not specify any VLAN, this command displays the historical port role calculation information of all VLANs. The displayed information is sorted by VLAN ID, and by port role calculation time in each VLAN.
- If you specify a VLAN, this command displays the historical port role calculation information of the specified VLAN by the sequence of port role calculation time.

Examples

# In MSTP mode, display the historical port role calculation information of IRF member switch 1 in MSTI 2.

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

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

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

# In PVST mode, display the historical port role calculation information of IRF member switch 1 in VLAN 2.

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

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

Table 29 Command output

Field	Description
Port	Port name.

Field	Description
Role change	Role change of the port ("Age" means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.
Port priority	Port priority.

display stp region-configuration

Syntax

display stp region-configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

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

Examples

# In MSTP mode, display effective MST region configuration information.

```
<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
```

# In PVST mode, display the effective MST region configuration information.

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

```
[Sysname] display stp region-configuration
 Oper Configuration
   Format selector      :0
   Region name          :hello
   Revision level       :0
   Configuration digest :0x5f762d9a46311effb7a488a3267fca9f

   Instance   Mode      Vlans Mapped
      0       default   3 to 4094
      1       static    1
      2       dynamic   2
```

Table 30 Command output

Field	Description
Format selector	Format selector 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, which can be configured by using the **revision-level** command and defaults to 0.
Mode	MSTI mode: • **Default**—The default instance MSTI 0. In PVST mode, the spanning tree feature is disabled. • **Static**—The static MSTI. • **Dynamic**—The dynamically assigned MSTI, which only exists in PVST mode.

display stp root

Syntax

display stp root [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

# In MSTP mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
 MSTID  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> system-view
[Sysname] stp mode pvst
[Sysname] display stp root
 VLAN  Root Bridge ID        ExtPathCost IntPathCost Root Port
    1  0.00e0-fc0e-6554      200200      0           GigabitEthernet1/0/1
```

Table 31 Command output

Field	Description
ExtPathCost	External path cost. The device automatically calculates the default path cost of a port. Or, you can use the **stp cost** command to configure the path cost of a port.
IntPathCost	Internal path cost. The device automatically calculates the default path cost of a port. Or, you can use the **stp cost** command to configure the path cost of a port.
Root Port	Root port name (displayed only if a port of the device is the root port of MSTIs).

display stp tc

Syntax

display stp [**instance** *instance-id* | **vlan** *vlan-id*] **tc** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

0: Visit level

Parameters

instance *instance-id*: Displays the statistics of TC/TCN BPDUs received and sent by all ports in a particular MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

vlan *vlan-id*: Displays the statistics of TC/TCN BPDUs received and sent by all ports in the specified VLAN, in the range of 1 to 4094.

slot *slot-number*: Displays the statistics of TC/TCN BPDUs received and sent by all ports on the specified IRF member switch. *slot-number* represents the member number of the device in the IRF. If this keyword-argument combination is not specified, this command displays the statistics of TC/TCN BPDUs received and sent by all ports on all IRF member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

In STP/RSTP mode, the displayed information is sorted by port name.

In MSTP mode, follow these guidelines:

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

In PVST mode, follow these guidelines:

- If you do not specify any VLAN, this command displays the statistics of TC/TCN BPDUs received and sent by all ports in all VLANs. The displayed information is sorted by VLAN ID and by port name in each VLAN.
- If you specify a VLAN, this command displays the statistics of TC/TCN BPDUs received and sent by all ports in the specified VLAN, in port name order.

Examples

# In MSTP mode, display the statistics of TC/TCN BPDUs received and sent by all ports on IRF member switch 1 in MSTI 0.

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

# In PVST mode, display the statistics of TC/TCN BPDUs received and sent by all ports on IRF member switch 1 in VLAN 2.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 VLAN      Port                      Receive      Send
    2      GigabitEthernet1/0/1         6           4
    2      GigabitEthernet1/0/2         0           2
```

Table 32 Command output

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

instance

Syntax

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

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

View

MST region view

Default level

2: System level

Parameters

instance-id: Specifies an MSTI ID. The minimum value is 0, representing the CIST.

- In MSTP mode, the *instance-id* argument ranges from 0 to 16.
- In PVST mode, the *instance-id* argument ranges from 0 to 32.

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

Use **instance** to map a list of VLANs to the specified MSTI.

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

By default, all VLANs are mapped to the CIST.

If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified MSTI will be remapped to the CIST.

You cannot map the same VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping will be automatically removed.

In PVST mode, you can map multiple VLANs to the CIST, and only one VLAN to each remaining MSTI.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

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

Examples

# Map VLAN 2 to MSTI 1.

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

region-name

Syntax

region-name *name*

undo region-name

View

MST region view

Default level

2: System level

Parameters

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

Description

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

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

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

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, run the **active region-configuration** command to activate the configured MST region name.

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

Examples

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

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

reset stp

Syntax

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

View

User view

Default level

1: Monitor level

Parameters

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

Description

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

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

If you specify the *interface-list* argument, the **reset stp** command clears the spanning tree-related statistics on the specified ports. Without the argument, the **reset stp** command clears the spanning tree-related statistics on all ports.

Related commands: **display stp**.

Examples

# Clear the spanning tree-related 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
```

revision-level

Syntax

revision-level *level*

undo revision-level

View

MST region view

Default level

2: System level

Parameters

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

Description

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

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

By default, the MSTP revision level is 0.

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region. When the MST region name and VLAN-to-instance mapping table are both the same for two MST regions, they can still be differentiated by their MSTP revision levels.

After configuring this command, run the **active region-configuration** command to activate the configured MST region level.

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

Examples

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

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

stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

View

System view

Default level

2: System level

Parameters

None

Description

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

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

By default, the BPDU guard function is disabled.

Examples

# Enable the BPDU guard function.

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

stp bridge-diameter

Syntax

stp [**vlan** *vlan-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-list*] **bridge-diameter**

View

System view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

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

Description

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

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

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

An appropriate setting of hello time, forward delay, and max age can speed up network convergence. The values of these timers are related to the network size and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers will also be set to their defaults.

To set the network diameter of an STP/RSTP/MSTP switched network, use this command without specifying any VLAN. To set the network diameter of a specified VLAN or multiple VLANs in a PVST switched network, use this command with a VLAN list specified.

In STP, RSTP, or MSTP mode, each MST region is considered as a device, and the configured network diameter of the switched network is only effective for the CIST (or the common root bridge), not for MSTIs.

In PVST mode, the network diameter configuration takes effect only on the root bridge.

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

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 to 5.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp vlan 2 bridge-diameter 5
```

stp compliance

Syntax

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

undo stp compliance

View

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

Default level

2: System level

Parameters

auto: Configures the ports to recognize the MSTP BPDU format automatically and determine the format of MSTP BPDUs to send.

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

legacy: Configures the ports to receive and send only compatible-format MSTP BPDUs.

Description

Use **stp compliance** to configure the mode the specified ports will use to recognize and send MSTP BPDUs.

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

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

Configured in Ethernet interface view, the setting takes effect on that interface only.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

Examples

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

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

stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

View

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

Default level

2: System level

Parameters

None

Description

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

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

The feature is disabled by default.

Configured in system view, the setting takes effect globally.

Configured in Ethernet interface view, the setting takes effect on the interface only.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

Enable this feature both globally and on ports connected to other vendors' devices to make it effective. To minimize impact, enable the feature on all associated ports before you enable it globally.

Related commands: **display stp**.

Examples

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

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

stp cost

Syntax

stp [**instance** *instance-id* | **vlan** *vlan-list*] **cost** *cost*

undo stp [**instance** *instance-id* | **vlan** *vlan-list*] **cost**

View

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

Default level

2: System level

Parameters

instance *instance-id*: Sets the path cost of the ports in a particular MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

cost: Specifies the path cost of the port, with an effective range that depends on the path cost calculation standard adopted.

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

Description

Use **stp cost** to set the path cost of the port or ports.

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

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

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

To set the path cost of an MSTP port in a specific MSTI, use this command with the MSTI specified. To set the path cost of a PVST port in a specific VLAN, use this command with the VLAN specified. To set the path cost of an MSTP port in the CIST or an STP/RSTP port, use this command without specifying any MSTI and VLAN.

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, which 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 will re-calculate the role of the port and initiate a state transition.

Related commands: **display stp** and **stp pathcost-standard**.

Examples

# In MSTP mode, set the path cost of port GigabitEthernet 1/0/3 in MSTI 2 to 200.

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

# In PVST mode, set the path cost of port GigabitEthernet 1/0/3 in VLAN 2 to 200.

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

stp edged-port

Syntax

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

undo stp edged-port

View

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

Default level

2: System level

Parameters

enable: Configures the ports as edge ports.

disable: Configures the ports as non-edge ports.

Description

Use **stp edged-port enable** to configure the ports as edge ports.

Use **stp edged-port disable** to configure the ports as non-edge ports.

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

By default, all ports are non-edge ports.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. You can enable the port to transition to the forwarding state rapidly by configuring it as an edge port. HP recommends you to configure ports directly connecting 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. Therefore, if a port receives a configuration BPDU when the BPDU guard function is disabled, the port functions as a non-edge port, even if you configure it as an edge port.

You cannot configure edge port settings and loop guard on a port at the same time.

Related commands: **stp loop-protection**.

Examples

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

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

stp enable

Syntax

In system view:

stp [**vlan** *vlan-list*] **enable**

undo stp [**vlan** *vlan-list*] **enable**

In Ethernet interface, Layer 2 aggregate interface, port group:

stp enable

undo stp enable

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

Use **stp enable** to enable the spanning tree feature globally.

Use **undo stp enable** to disable the spanning tree feature.

By default, the spanning tree feature is disabled globally, enabled on all VLANs, and enabled on all ports.

To enable or disable the spanning tree feature globally (not for any VLANs), use this command without specifying any VLAN in system view. To enable or disable the spanning tree feature on specific VLANs, use this command with the VLANs specified in system view.

Configured in system view, the setting takes effect globally.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

When you enable the spanning tree feature, the device operates in STP-compatible, RSTP, MSTP, or PVST mode, depending on the spanning tree mode setting.

When you enable MSTP, the switch dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs.

When you disable MSTP, the switch stops maintaining the spanning tree status.

Related commands: **stp mode**.

Examples

# In MSTP mode, enable the spanning tree feature globally.

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

# In PVST mode, enable the spanning tree feature globally and in VLAN 2.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp enable
[Sysname] stp vlan 2 enable
```

# In MSTP mode, disable the spanning tree feature on port GigabitEthernet 1/0/1.

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

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

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

Default level

2: System level

Parameters

None

Description

Use **stp loop-protection** to enable the loop guard function on the ports.

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

By default, the loop guard function is disabled.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

You cannot configure edge port settings and loop guard, or configure root guard and loop guard on a port at the same time.

Related commands: **stp edged-port** and **stp root-protection**.

Examples

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

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

stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

View

System view

Default level

2: System level

Parameters

hops: Sets the maximum hops, in the range of 1 to 40.

Description

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

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

By default, the maximum number of hops of an MST region is 20.

Related commands: **display stp**.

Examples

# Set the maximum hops of the MST region to 35.

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

stp mcheck

Syntax

stp mcheck

View

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

Default level

2: System level

Parameters

None

Description

Use **stp mcheck** to perform the mCheck operation globally or on a port.

If a port on a device running MSTP, RSTP, or PVST mode connects to an STP device, the port will automatically migrate to the STP-compatible mode. It will not be able to migrate automatically back to the MSTP, RSTP, or PVST mode, so it will remain operating in the STP-compatible mode until the STP switch is shut down or removed, or migrated to the MSTP, RSTP, or PVST mode. Then, you can perform an mCheck operation to force the port to migrate to the MSTP, RSTP, or PVST mode.

Suppose Device A running STP, Device B with no spanning tree feature enabled, and Device C running RSTP or MSTP are connected in order. Device B will transparently transmit the STP BPDUs, and the port on Device C and connecting to Device B will transition to the STP mode. After you enable the spanning tree feature on Device B, to run RSTP or MSTP between Device B and Device C, you must perform an mCheck operation on the ports interconnecting Device B and Device C, in addition to configuring the spanning tree to operate in RSTP or MSTP mode on Device B.

The device operates in STP-compatible, RSTP, MSTP, or PVST mode depending on the spanning tree mode setting.

The **stp mcheck** command is effective only when the device operates in MSTP, RSTP, or PVST mode.

Configured in system view, the setting takes effect globally.

Configured in Ethernet interface view, the setting takes only effect on the interface.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

Related commands: **stp mode**.

Examples

# Perform mCheck on GigabitEthernet 1/0/1.

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

stp mode

Syntax

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

undo stp mode

View

System view

Default level

2: System level

Parameters

stp: Configures the spanning tree device to operate in STP-compatible mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

Description

Use **stp mode** to configure the spanning tree operating mode.

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

By default, a spanning tree device operates in MSTP mode.

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

Examples

# Configure the spanning tree device to operate in STP-compatible mode.

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

stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

View

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

Default level

2: System level

Parameters

None

Description

Use **stp no-agreement-check** to enable No Agreement Check on the ports.

Use **undo stp no-agreement-check** to disable No Agreement Check on the ports.

By default, No Agreement Check is disabled.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all member ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

This feature takes effect only after you enable it on the root port.

Examples

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

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

stp pathcost-standard

Syntax

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

undo stp pathcost-standard

View

System view

Default level

2: System level

Parameters

dot1d-1998: 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.

Description

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.

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

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

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

Examples

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

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

stp point-to-point

Syntax

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

undo stp point-to-point

View

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

Default level

2: System level

Parameters

auto: Specifies automatic detection of the link type.

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

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

Description

Use **stp point-to-point** to configure the link type of the ports.

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

The default setting is **auto** and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all member ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

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. HP recommends that you use the default setting, which lets the device automatically detect the port link type.

The **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port in MSTP or PVST mode is effective for all MSTIs or VLANs.

If the physical link to which the port connects is not a point-to-point link but you set it to be one, the configuration may bring a temporary loop.

Related commands: **display stp**.

Examples

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

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

stp port priority

Syntax

stp [**instance** *instance-id* | **vlan** *vlan-list*] **port priority** *priority*

undo stp [**instance** *instance-id* | **vlan** *vlan-list*] **port priority**

View

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

Default level

2: System level

Parameters

instance *instance-id*: Sets the priority of the ports in a particular MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

priority: Specifies a port priority, in the range of 0 to 240 in steps of 16 (as in 0, 16, 32).

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

Use **stp port priority** to set the priority of the ports.

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

By default, the port priority is 128.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

To set the priority of an MSTP port in a specific MSTI, use this command with the MSTI specified. To set the priority of a PVST port in a specific VLAN or multiple VLANs, use this command with a VLAN list specified. To set the priority of an MSTP port in the CIST or an STP/RSTP port, use this command without specifying any MSTI and VLAN.

Port priority affects the role of a port in a spanning tree.

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.

Related commands: **display stp**.

Examples

# In MSTP mode, set the priority of port GigabitEthernet 1/0/3 to 16 in MSTI 2.

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

# In PVST mode, set the priority of port GigabitEthernet 1/0/3 to 16 in VLAN 2.

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

stp port-log

Syntax

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

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

View

System view

Default level

2: System level

Parameters

instance *instance-id*: Specifies an MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST. To enable or disable outputting port state transition information in STP/RSTP mode, specify **instance 0**.

all: Specifies all MSTIs.

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

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

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

By default, this function is enabled.

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   2006   Sysname   MSTP/3/MSTP_DISCARDING:   Instance   2's
GigabitEthernet1/0/1 has been set to discarding state!
%Aug   16   00:49:41:856   2006   Sysname   MSTP/3/MSTP_DISCARDING:   Instance   2's
GigabitEthernet1/0/2 has been set to forwarding state!
```

The output shows that GigabitEthernet 1/0/1 in MSTI 2 transitioned to the discarding state and GigabitEthernet 1/0/2 in MSTI 2 transitioned to the forwarding state.

# In PVST mode, enable outputting port state transition information for VLAN 1 to VLAN 4094.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PVST_DISCARDING: VLAN 2's GigabitEthernet1/0/1
has been set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PVST_FORWARDING: VLAN 2's GigabitEthernet1/0/2
has been set to forwarding state!
```

The output shows that GigabitEthernet 1/0/1 in VLAN 2 transitioned to the discarding state and GigabitEthernet 1/0/2 in VLAN 2 transitioned to the forwarding state.

stp priority

Syntax

stp [**instance** *instance-id* | **vlan** *vlan-list*] **priority** *priority*

undo stp [**instance** *instance-id* | **vlan** *vlan-list*] **priority**

View

System view

Default level

2: System level

Parameters

instance *instance-id*: Sets the priority of the device in an MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

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

priority: Specifies a 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.

Description

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

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

By default, the device priority is 32768.

To set the priority of an MSTP device in a specific MSTI, use this command with the MSTI specified. To set the priority of a PVST device in a specific VLAN or multiple VLANs, use this command with a VLAN list specified. To set the priority of an MSTP device in the CIST or an STP/RSTP device, use this command without specifying any MSTI and VLAN.

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 mode pvst
[Sysname] stp vlan 1 priority 4096
```

stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

View

System view

Default level

2: System level

Parameters

None

Description

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

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

These are the default settings for the MST region:

- The MST region name of the device is the MAC address of the device.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

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

Examples

# Enter MST region view.

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

stp root primary

Syntax

stp [**instance** *instance-id* | **vlan** *vlan-list*] **root primary**

undo stp [**instance** *instance-id* | **vlan** *vlan-list*] **root**

View

System view

Default level

2: System level

Parameters

instance *instance-id*: Configures the device as the root bridge in a particular MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

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

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

By default, a device is not a root bridge.

To set an MSTP device as the root bridge in a specific MSTI, use this command with the MSTI specified. To set a PVST device as the root bridge in a specific VLAN or multiple VLANs, use this command with a VLAN list specified. To set an MSTP device in the CIST or an STP/RSTP device as the root bridge, use this command without specifying any MSTI and VLAN.

Once you specify the device as the root bridge, you cannot change the priority of the device.

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

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 mode pvst
[Sysname] stp vlan 1 root primary
```

stp root secondary

Syntax

stp [**instance** *instance-id* | **vlan** *vlan-list*] **root secondary**

undo stp [**instance** *instance-id* | **vlan** *vlan-list*] **root**

View

System view

Default level

2: System level

Parameters

instance *instance-id*: Configures the device as a secondary root bridge in a particular MSTI. The value of *instance-id* ranges from 0 to 16, where 0 represents the CIST.

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

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

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

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

To set an MSTP device as a secondary root bridge in a specific MSTI, use this command with the MSTI specified. To set a PVST device as a secondary root bridge in a specific VLAN or multiple VLANs, use this command with a VLAN list specified. To set an MSTP device in the CIST or an STP/RSTP device as a secondary root bridge, use this command without specifying any MSTI and VLAN.

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

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

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 mode pvst
[Sysname] stp vlan 1 root secondary
```

stp root-protection

Syntax

stp root-protection

undo stp root-protection

View

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

Default level

2: System level

Parameters

None

Description

Use **stp root-protection** to enable the root guard function on the ports.

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

By default, the root guard function is disabled.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

You cannot configure root guard and loop guard on a port at the same time.

Related commands: **stp loop-protection**.

Examples

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

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

stp tc-protection

Syntax

stp tc-protection enable

stp tc-protection disable

View

System view

Default level

2: System level

Parameters

None

Description

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

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

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

Examples

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

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

stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

View

System view

Default level

2: System level

Parameters

number: Sets the maximum number of immediate forwarding address entry flushes that the device can perform within a certain period of time (10 seconds). The value ranges from 1 to 255.

Description

Use **stp tc-protection threshold** to configure the maximum number of forwarding address entry flushes that the device can perform every a certain period of time (10 seconds).

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

By default, the device can perform a maximum of six forwarding address entry flushes every 10 seconds.

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
```

stp tc-snooping

Syntax

stp tc-snooping

undo stp tc-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **stp tc-snooping** to enable topology change (TC) snooping.

Use **undo stp tc-snooping** to disable TC snooping.

By default, TC snooping disabled.

TC snooping and STP are mutually exclusive. Before enabling TC snooping, first disable STP globally.

TC snooping does not take effect on the ports on which BPDU tunneling is enabled for STP. For more information about BPDU tunneling, see *Layer 2—LAN Switching Configuration Guide*.

Related commands: **stp enable**.

Examples

# Enable TC snooping globally.

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

stp timer forward-delay

Syntax

stp [**vlan** *vlan-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-list*] **timer forward-delay**

View

System view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

time: Sets the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Description

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

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

By default, the forward delay timer is 1500 centiseconds.

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 transitions from the discarding to the forwarding state. To stay synchronized with the remote device, the port has a wait period between transition states that is determined by the forward delay timer.

To set the forward delay in STP/RSTP/MSTP mode, use this command without any VLAN specified. To set the forward delay for a specific VLAN or multiple VLANs in PVST mode, use this command with a VLAN list specified.

HP does not recommend that you 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 and let spanning tree protocols automatically calculate optimal settings of the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

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

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 to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp vlan 2 timer forward-delay 2000
```

stp timer hello

Syntax

stp [**vlan** *vlan-list*] **timer hello** *time*

undo stp [**vlan** *vlan-list*] **timer hello**

View

System view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

time: Sets the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Description

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

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

By default, the hello time is 200 centiseconds.

Hello time is the time interval at which spanning tree devices send configuration BPDUs to maintain spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process will be triggered due to timeout.

To set the hello time in STP/RSTP/MSTP mode, use this command without any VLAN specified. To set the hello time for a specific VLAN or multiple VLANs in PVST mode, use this command with a VLAN list specified.

HP does not recommend that you 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 and let spanning tree protocols automatically calculate optimal settings of the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

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

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 in VLAN 2 to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp vlan 2 timer hello 400
```

stp timer max-age

Syntax

stp [**vlan** *vlan-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-list*] **timer max-age**

View

System view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the VLAN ID, in the range of 1 to 4094, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

time: Sets the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Description

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

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

By default, the max age is 2000 centiseconds.

In the CIST of an MSTP network or each VLAN of a PVST network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If yes, a new spanning tree calculation process starts. The max age timer is ineffective for MSTIs.

To set the max age timer in STP/RSTP/MSTP mode, use this command without any VLAN specified. To set the max age timer for a specific VLAN or multiple VLANs in PVST mode, use this command with a VLAN list specified.

HP does not recommend that you 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 and let spanning tree protocols automatically calculate optimal settings of the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Related commands: **stp timer forward-delay**, **stp timer hello**, and **stp bridge-diameter**.

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 in VLAN 2 to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp vlan 2 timer max-age 1000
```

stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

View

System view

Default level

2: System level

Parameters

factor: Sets the timeout factor, in the range of 1 to 20.

Description

Use **stp timer-factor** to configure the timeout time by setting the timeout factor.

Timeout time = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

By default, the timeout factor of the switch is set to 3.

After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the surrounding devices at the interval of hello time to check whether any link is faulty. If a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.

In a stable network, this kind of spanning tree calculation may occur because the upstream device is busy. You can avoid such unwanted spanning tree calculations by lengthening the timeout time (by setting the timeout factor to 4 or more), saving the network resources. HP recommends you to set the timeout factor to 5, 6, or 7 for a stable network.

Related commands: **stp timer hello**.

Examples

# Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

View

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

Default level

2: System level

Parameters

limit: Sets the maximum number of BPDUs the ports can send within each hello time, in the range of 1 to 255.

Description

Use **stp transmit-limit** to set the maximum number of BPDUs that the ports can send within each hello time.

Use **undo stp transmit-limit** to restore the default.

By default, the maximum transmission rate of all ports is 10. Each port can send up to 10 BPDUs within each hello time.

Configured in Ethernet interface view, the setting takes effect only on the interface.

Configured in port group view, the setting takes effect on all member ports in the port group.

Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface.

Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group.

A larger maximum transmission rate value requires more system resources. An appropriate maximum transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. HP recommends that you use the default value.

Examples

# Set the maximum transmission rate of port GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

View

MST region view

Default level

2: System level

Parameters

modulo: Sets the modulo value, in the range of 1 to 16.

Description

Use **vlan-mapping modulo** to map VLANs in the MST region to MSTIs according to the specified modulo value, quickly creating a VLAN-to-instance mapping table.

By default, all VLANs are mapped to the CIST (MSTI 0).

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 will be automatically removed.

This command maps each VLAN to the MSTI whose ID is (VLAN ID - 1) %*modulo* + 1, where (VLAN ID - 1) %*modulo* is the modulo operation for (VLAN ID - 1). If the modulo value is 15, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 15 to MSTI 15, VLAN 16 to MSTI 1, and so on.

Related commands: **region-name**, **revision-level**, **display stp region-configuration**, **check region-configuration**, and **active region-configuration**.

Examples

# Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

BPDU tunneling configuration commands

bpdu-tunnel dot1q

Syntax

In Layer 2 Ethernet interface view or port group view:

bpdu-tunnel dot1q { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }

undo bpdu-tunnel dot1q { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }

In Layer 2 aggregate interface view:

bpdu-tunnel dot1q { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** }

undo bpdu-tunnel dot1q { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** }

View

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

Default level

2: System level

Parameters

cdp: Specifies the Cisco Discovery Protocol (CDP).

dldp: Specifies the Device Link Detection Protocol (DLDP).

eoam: Specifies Ethernet Operation, Administration and Maintenance (EOAM).

gvrp: Specifies the GARP VLAN Registration Protocol (GVRP).

hgmp: Specifies the HW Group Management Protocol (HGMP).

lacp: Specifies the Link Aggregation Control Protocol (LACP).

lldp: Specifies the Link Layer Discovery Protocol (LLDP).

pagp: Specifies the Port Aggregation Protocol (PAGP).

pvst: Specifies Per VLAN Spanning Tree (PVST).

stp: Specifies the Spanning Tree Protocol (STP).

udld: Specifies Unidirectional Link Direction (UDLD).

vtp: Specifies the VLAN Trunking Protocol (VTP).

Description

Use **bpdu-tunnel dot1q** to enable BPDU tunneling for a protocol on the port(s).

Use **undo bpdu-tunnel dot1q** to disable BPDU tunneling for a protocol on the port(s).

By default, BPDU tunneling for any protocol is disabled.

Settings made in Layer 2 Ethernet interface view or Layer 2 aggregate interface view take effect only on the Ethernet interface or aggregate interface. Settings made in port group view take effect on all ports in the port group.

Before enabling BPDU tunneling for DLDP, EOAM, GVRP, HGMP, LLDP, or STP on a port, disable the protocol on the port first.

To enable BPDU tunneling for PVST (which is a spanning tree protocol) on a port, disable STP first and then enable BPDU tunneling for STP on the port.

Do not enable BPDU tunneling for DLDP, EOAM, LACP, LLDP, PAGP, or UDLD on the member port of a Layer 2 aggregation group.

Examples

# Disable STP on GigabitEthernet 1/0/1, and then enable BPDU tunneling for STP on the port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

# Disable STP for port group 1, and then enable BPDU tunneling for STP in the port group.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet
1/0/6
[Sysname-port-group-manual-1] undo stp enable
[Sysname-port-group-manual-1] bpdu-tunnel dot1q stp
```

# Disable STP on Layer 2 aggregate interface Bridge-Aggregation 1, and then enable BPDU tunneling for STP on the Layer 2 aggregate interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] bpdu-tunnel dot1q stp
```

bpdu-tunnel tunnel-dmac

Syntax

bpdu-tunnel tunnel-dmac *mac-address*

undo bpdu-tunnel tunnel-dmac

View

System view

Default level

2: System level

Parameters

mac-address: Specifies a destination multicast MAC address for BPDUs, in the format of H-H-H. The allowed values are 0x0100-0CCD-CDD0, 0x0100-0CCD-CDD1, 0x0100-0CCD-CDD2, and 0x010F-E200-0003.

Description

Use **bpdu-tunnel tunnel-dmac** to configure the destination multicast MAC address for BPDUs.

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

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

Examples

# Set the destination multicast MAC address for BPDUs to 0x0100-0CCD-CDD0.

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

VLAN configuration commands

Basic VLAN configuration commands

default

Syntax

default

View

VLAN interface view

Default level

2: System level

Parameters

None

Description

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

Use **default** to restore the default settings for a VLAN interface.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. You can use the **display this** command in interface view to check for these commands, and perform their **undo** forms or follow the command reference to individually restore their default settings. If your restoration attempt still fails, follow the error message 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
This command will restore the default settings. Continue? [Y/N]:y
```

description

Syntax

description *text*

undo description

View

VLAN view, VLAN interface view

Default level

2: System level

Parameters

text: Description of a VLAN or VLAN interface. The string can include case-sensitive letters, digits, special characters such as tilde (~), exclamation point (!), at sign (@), pound sign (#), dollar sign ($), percent sign (%), caret (^), ampersand sign (&), asterisk (*), left brace({), right brace (}), left parenthesis ((), right parenthesis ()), left bracket ([), right bracket (]), left angle bracket (<), right angle bracket (>), hyphen (-), underscore(_), plus sign (+), equal sign (=), vertical bar (|), back slash (\), colon (:), semi-colon (;) quotation marks ("), apostrophe ('), comma (,), dot (.), and slash (/), spaces, and other Unicode characters and symbols.

- For a VLAN, this is a string of 1 to 32 characters.
- For a VLAN interface, this is a string of 1 to 80 characters.

When you specify a description, follow these guidelines:

- Each Unicode character takes the space of two regular characters.
- To use Unicode characters or symbols in an interface description, install the specific input method editor and log in to the device through remote login software that supports the character type.
- When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.

Description

Use **description** to change the description of the VLAN or VLAN interface.

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

- The default description for a VLAN is the VLAN ID. For example, **VLAN 0001**.
- The default description for a VLAN interface is the name of the interface. For example, **Vlan-interface 1 Interface**.

You can configure a description to describe the function or connection of a VLAN or VLAN interface for easy management.

Examples

# Change the description of VLAN 2 to **sales-private**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
```

# Change the description of VLAN-interface 2 to **linktoPC56**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

display interface vlan-interface

Syntax

display interface [**vlan-interface**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface vlan-interface *vlan-interface-id* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-interface-id: Specifies a VLAN interface number.

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

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display interface vlan-interface** to display information about a specified or all VLAN interfaces.

If you do not provide the **vlan-interface** keyword, this command displays information about all interfaces.

If you provide the **vlan-interface** keyword but do not specify the VLAN interface number, this command displays information about all VLAN interfaces.

Related commands: **reset counters interface vlan-interface**.

Examples

# Display information for VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: DOWN
Line protocol current state: DOWN
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e249-8050
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e249-8050
Last clearing of counters:  Never
     Last 300 seconds input:  0 bytes/sec 0 packets/sec
     Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

# Display brief information for VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2 brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Vlan2                DOWN DOWN     --
```

# Display brief information for VLAN interfaces in DOWN state.

```
<Sysname> display interface vlan-interface brief down
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Vlan2                DOWN Not connected
```

Table 33 Command output

Field	Description
Vlan-interface2 current state	Physical state of a VLAN interface: • **DOWN (Administratively)**—The administrative state of the VLAN interface is down, because it has been shut down with the **shutdown** command. • **DOWN**—The administrative sate of the VLAN interface is up, but its physical sate is down. The VLAN corresponding to this interface does not contain any physical port in the UP state (possibly because the ports are not well connected or the lines have failed). • **UP**—Both the administrative state and the physical state of the VLAN interface are up.
Line protocol current state	Link layer protocol state of a VLAN interface: • **DOWN**—The protocol state of the VLAN interface is down. • **UP**—The protocol state of the VLAN interface is up.
Description	Description string of a VLAN interface.
The Maximum Transmit Unit	MTU of a VLAN interface.
Internet protocol processing : disabled	The interface is not capable of processing IP packets. This information is displayed when the interface is not configured with an IP address.
Internet Address is 192.168.1.54/24 Primary	The primary IP address of the interface is 192.168.1.54/24. This information is displayed only if the primary IP address is configured for the interface.
Internet Address is 6.4.4.4/24 Sub	The secondary IP address of the interface is 6.4.4.4/24. This information is displayed only if a secondary IP address is configured for the interface.
IP Packet Frame Type	IPv4 outgoing frame format.
Hardware address	MAC address corresponding to a VLAN interface.
IPv6 Packet Frame Type	IPv6 outgoing frame format.

Field	Description
Last clearing of counters	Time when the **reset counters interface vlan-interface** command was last used to clear the interface statistics. **Never** indicates the **reset counters interface** command has never been used on the interface since the device's startup.
Last 300 seconds input: 0 bytes/sec 0 packets/sec	Average rate of input packets in the last 300 seconds (in bps and pps).
Last 300 seconds output: 0 bytes/sec 0 packets/sec	Average rate of output packets in the last 300 seconds (in bps and pps).
0 packets input, 0 bytes, 0 drops	Total number and size (in bytes) of the received packets of the interface and the number of the dropped packets.
0 packets output, 0 bytes, 0 drops	Total number and size (in bytes) of the sent packets of the interface and the number of the dropped packets.
The brief information of interface(s) under route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link layer state of the interface: • **ADM**—The interface has been administratively shut down. To recover its physical state, perform the **undo shutdown** command. • **Stby**—The interface is operating as a standby interface.
Protocol: (s) - spoofing	If the network layer protocol state of an interface is shown as UP, but its link is an on-demand link or not present at all, its protocol attribute includes the spoofing flag (an s in parentheses).
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The link is up. • **ADM**—The link has been administratively shut down. To recover its physical state, perform the **undo shutdown** command.
Protocol	Protocol connection state of the interface, which can be UP, DOWN, or UP(s).
Main IP	Main IP address of the interface.
Description	Description of the interface.
Cause	Cause of a DOWN physical link. If the port has been shut down with the **shutdown** command, this field displays **Administratively**. To restore the physical state of the interface, use the **undo shutdown** command.

display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-id1: Displays information about a VLAN specified by VLAN ID, in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Displays information about VLANs specified by a VLAN ID range.

all: Displays all VLAN information but the reserved VLANs.

dynamic: Displays the number of dynamic VLANs and the ID for each dynamic VLAN. The dynamic VLANs are generated through GVRP or those distributed by a RADIUS server.

reserved: Displays information about the reserved VLANs. Protocol modules determine which VLANs are reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. You cannot configure reserved VLANs.

static: Displays the number of static VLANs and the ID for each static VLAN. The static VLANs are manually created.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display vlan** to display VLAN information.

Related commands: **vlan**.

Examples

# Display VLAN 2 information.

```
<Sysname> display vlan 2
VLAN ID: 2
 VLAN Type: static
 Route interface: not configured
 Description: VLAN 0002
 Name: VLAN 0002
Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

# Display VLAN 3 information.

```
<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
 IPv6 global unicast address(es):
    2001::1, subnet is 2001::/64 [TENTATIVE]
```

```
Description: VLAN 0003
 Name: VLAN 0003
 Tagged   Ports: none
 Untagged Ports: none
```

Table 34 Command output

Field	Description
VLAN Type	VLAN type, static or dynamic.
Route interface	Indicates whether the VLAN interface is configured or not.
Description	Description of the VLAN.
Name	Name configured for the VLAN.
IPv4 address	Primary IPv4 address of the VLAN interface (available only when an IPv4 address is configured for the VLAN interface). To display secondary IP addresses, use the **display interface vlan-interface** command in any view or the **display this** command in VLAN interface view.
IPv4 subnet mask	Subnet mask of the primary IPv4 address (available only when an IPv4 address is configured for the VLAN interface).
IPv6 global unicast address(es)	Global unicast IPv6 address of the VLAN interface (available only when an IPv6 address is configured for the VLAN interface).
Tagged Ports	Ports through which VLAN packets are sent tagged.
Untagged Ports	Ports through which VLAN packets are sent untagged.

interface vlan-interface

Syntax

interface vlan-interface *vlan-interface-id*

undo interface vlan-interface *vlan-interface-id*

View

System view

Default level

2: System level

Parameters

vlan-interface-id: Specifies a VLAN interface number, in the range of 1 to 4094.

Description

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 remove the specified VLAN interface.

Create the VLAN before you create the VLAN interface.

To configure an IP address for a VLAN interface that will perform IP routing, use the **ip address** command in VLAN interface view.

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

Examples

# Create VLAN-interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View

VLAN interface view

Default level

2: System level

Parameters

ip-address: Specifies an IP address in dotted decimal notation.

mask: Specifies a subnet mask in dotted decimal notation.

mask-length: Sets the number of consecutive 1s in the subnet mask, in the range of 0 to 32.

sub: Indicates the address is a secondary IP address.

Description

Use **ip address** to assign an IP address and subnet mask to a VLAN interface.

Use **undo ip address** to remove the IP address and subnet mask for a VLAN interface.

By default, no IP address is assigned to any VLAN interface.

To connect a VLAN to multiple subnets, assign one primary IP address and multiple secondary IP addresses to a VLAN interface.

When you configure IP addresses for a VLAN interface, follow these rules:

- The primary IP address you assign to a VLAN interface overwrites the previous one, if any.
- Remove all secondary IP addresses before you remove the primary IP address.
- To remove all IP addresses, use the **undo ip address** command without any parameter.
- To remove the primary IP address, use the **undo ip address** *ip-address* { *mask* | *mask-length* } command.
- To remove a secondary IP address, use the **undo ip address** [*ip-address* { *mask* | *mask-length* } [**sub**]] command

Related commands: **display ip interface** (*Layer 3—IP Services Command Reference*).

Examples

# Specify the IP address as 1.1.0.1, the subnet mask as 255.255.255.0 for VLAN interface 1.

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

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.0.1 255.255.255.0
```

mtu

Syntax

mtu *size*

undo mtu

View

VLAN interface view

Default level

2: System level

Parameters

size: Sets the maximum transmission unit (MTU), in the range of 46 to 1500 bytes.

Description

Use **mtu** to set the MTU for a VLAN interface.

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

By default, the MTU of a VLAN interface is 1500 bytes.

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

Examples

# Set the MTU to 1492 bytes for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mtu 1492
```

name

Syntax

name *text*

undo name

View

VLAN view

Default level

2: System level

Parameters

text: Specifies a VLAN name, a string of 1 to 32 characters. The string can include case-sensitive letters, digits, special characters such as tilde (~), exclamation point (!), at sign (@), pound sign (#), dollar sign ($), percent sign (%), caret (^), ampersand sign (&), asterisk (*), left brace({), right brace (}), left parenthesis ((), right parenthesis ()), left bracket ([), right bracket (]), left angle bracket (<), right angle bracket (>), hyphen (-), underscore(_), plus sign (+), equal sign (=), vertical bar (|), back slash (\), colon

(:), semi-colon (;) quotation marks ("), apostrophe ('), comma (,), dot (.), and slash (/), spaces, and other Unicode characters and symbols.

Description

Use **name** to configure a name for the VLAN.

Use **undo name** to restore the default name of the VLAN.

By default, the name of a VLAN is its VLAN ID, for example, **VLAN 0001**.

When 802.1X or MAC address authentication is configured on a switch, you can use a RADIUS server to issue VLAN configuration to ports that have passed the authentication. Some servers can send IDs or names of the issued VLANs to the switch.

Use VLAN names rather than VLAN IDs to distinguish a large number of VLANs.

Examples

# Configure the name of VLAN 2 as **Test VLAN**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name Test VLAN
```

reset counters interface vlan-interface

Syntax

reset counters interface vlan-interface [*vlan-interface-id*]

View

User view

Default level

2: System level

Parameters

vlan-interface-id: Specifies a VLAN interface number.

Description

Use **reset counters interface vlan-interface** to clear the statistics on a VLAN interface.

Before collecting the traffic statistics within a specific period of time on an interface, clear the existing statistics first.

If the *vlan-interface-id* argument is not specified, this command clears the statistics of all VLAN interfaces.

If the *vlan-interface-id* argument is specified, this command clears the statistics of the specified VLAN interface.

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

Examples

# Clear the statistics on VLAN-interface 2.

```
<Sysname> reset counters interface vlan-interface 2
```

shutdown

Syntax

shutdown

undo shutdown

View

VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

By default, a VLAN interface is up unless all ports in the VLAN are down.

Use **undo shutdown** to bring up a VLAN interface after configuring related parameters and protocols for the VLAN interface. You can shut down a failed VLAN interface with the **shutdown** command and then bring it up with the **undo shutdown** command to see if it recovers.

In a VLAN, the state of any 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

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

System view

Default level

2: System level

Parameters

vlan-id1, *vlan-id2*: Specifies a VLAN ID, in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range.

all: Creates or removes all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Description

Use **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 in the range of *vlan-id1* to *vlan-id2*, except reserved VLANs.

Use **undo vlan** to remove the specified VLANs.

You cannot create or remove the default VLAN (VLAN 1).

You cannot create or remove reserved VLANs reserved for specific functions.

For the following VLANs, you must remove the related configurations first, because you cannot use the **undo vlan** command to directly remove them:

- Protocol reserved VLANs
- Voice VLANs
- Management VLANs
- Dynamic VLANs
- VLANs configured with QoS policies
- Control VLANs configured for smart link groups or RRPP domains
- Remote probe VLANs for remote port mirroring

Related commands: **display vlan**.

Examples

# Enter VLAN 2 view.

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

# Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait............. Done.
```

Port-based VLAN configuration commands

display port

Syntax

display port { **hybrid** | **trunk** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

hybrid: Displays hybrid ports.

trunk: Displays trunk ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port** to display information about the hybrid or trunk ports on the device, including the port names, PVIDs, and allowed VLAN IDs.

Examples

# Display information about the hybrid ports in the system.

```
<Sysname> display port hybrid
Interface            PVID  VLAN passing
GE1/0/4               100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

# Display information about the trunk ports in the system.

```
<Sysname> display port trunk
Interface            PVID  VLAN passing
GE1/0/8               2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 35 Command output

Field	Description
Interface	Port name
PVID	PVID of the port
VLAN passing	VLANs for which the port allows packets to pass through
Tagged	VLANs for which the port sends packets without removing VLAN tags
Untagged	VLANs for which the port sends packets after removing VLAN tags

port

Syntax

port *interface-list*

undo port *interface-list*

View

VLAN view

Default level

2: System level

Parameters

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

Description

Use **port** to assign the specified access ports to the VLAN.

Use **undo port** to remove the specified access ports from the VLAN.

By default, all ports are in VLAN 1.

This command is only applicable on access ports.

By default, all ports are access ports. However, you can manually configure the port type. For more information, see "port link-type."

You cannot assign Layer 2 aggregate interfaces to a VLAN.

Related commands: **display vlan**.

Examples

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

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

View

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

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Verify that the VLAN specified by the VLAN ID already exists.

Description

Use **port access vlan** to assign the access ports to the specified VLAN.

Use **undo port access vlan** to restore the default.

By default, all access ports belong to VLAN 1.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

Examples

# Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

# Assign Layer 2 aggregate interface Bridge-Aggregation 1 and its member ports to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port access vlan 3
```

port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

View

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

Default level

2: System level

Parameters

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

Description

Use **port hybrid pvid** to configure the PVID of the hybrid port.

Use **undo port hybrid pvid** to restore the default.

By default, the PVID of a hybrid port is VLAN 1.

You can use a nonexistent VLAN as the PVID for a hybrid port. If you use the **undo vlan** command to remove the PVID of a hybrid port, it does not affect the setting of the PVID on the port.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.

- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

HP recommends that you set the same PVID for the local and remote hybrid ports.

You must use the **port hybrid vlan** command to configure the hybrid port to allow and forward packets from the PVID.

Related commands: **port link-type** and **port hybrid vlan**.

Examples

# Configure VLAN 100 as the PVID of the hybrid port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
```

# Configure VLAN 100 as the PVID of the hybrid Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid pvid vlan 100
```

port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View

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

Default level

2: System level

Parameters

vlan-id-list: Specifies a list of VLANs that the hybrid ports will be assigned to, in the format of [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges. Verify that the specified VLANs already exist.

tagged: Configures the port(s) to send tagged packets of the specified VLAN(s).

untagged: Configures the port(s) to send untagged packets of the specified VLAN(s).

Description

Use **port hybrid vlan** to assign the hybrid ports to the specified VLANs.

Use **undo port hybrid vlan** to remove the hybrid ports from the specified VLANs.

By default, a hybrid port only allows packets from VLAN 1 to pass through untagged.

A hybrid port can carry multiple VLANs. If you execute the **port hybrid vlan** command multiple times, the VLANs the hybrid port carries are the set of VLANs specified by *vlan-id-list* in each execution.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

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

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

# Assign hybrid ports in port group 2 to VLAN 2, and configure these hybrid ports to send packets of VLAN 2 with VLAN tags removed.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] port-group manual 2
[Sysname-port-group-manual-2] group-member gigabitethernet 1/0/1 to gigabitethernet
1/0/6
[Sysname-port-group-manual-2] port link-type hybrid
[Sysname-port-group-manual-2] port hybrid vlan 2 untagged
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
 Configuring GigabitEthernet1/0/4... Done.
 Configuring GigabitEthernet1/0/5... Done.
 Configuring GigabitEthernet1/0/6... Done.
```

# Assign the hybrid Layer 2 aggregate interface Bridge-Aggregation 1 and its member ports to VLAN 2, and configure them to send packets of VLAN 2 with tags removed.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done.
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
```

The output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are the member ports of the aggregation group corresponding to Bridge-Aggregation 1.

port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

View

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

Default level

2: System level

Parameters

access: Configures the link type of a port as access.

hybrid: Configures the link type of a port as hybrid.

trunk: Configures the link type of a port as trunk.

Description

Use **port link-type** to configure the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

By default, any port is an access port.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access.

After you change the link type of an interface with the **port link-type** command, the loopback detection action configured on the interface with the **loopback-detection action** command automatically restores the default. For more information about the loopback detection action configuration, see *Layer 2—LAN Switching Configuration Guide*.

Examples

# Configure GigabitEthernet 1/0/1 as a trunk port.

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

# Configure all the ports in the manual port group **group1** as hybrid ports.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member gigabitethernet 1/0/1
[Sysname-port-group manual group1] group-member gigabitethernet 1/0/2
[Sysname-port-group manual group1] port link-type hybrid
```

# Configure Layer 2 aggregate interface Bridge-Aggregation 1 and its member ports as hybrid ports.

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

port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View

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

Default level

2: System level

Parameters

vlan-id-list: Specifies a list of VLANs that the trunk ports will be assigned to, in the format of [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* is in the range of 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

all: Permits all VLANs to pass through the trunk ports.

Description

Use **port trunk permit vlan** to assign the trunk ports to the specified VLANs.

Use **undo port trunk permit vlan** to remove the trunk ports from the specified VLANs.

By default, a trunk port allows only packets from VLAN 1 to pass through.

A trunk port can carry multiple VLANs. If you execute the **port trunk permit vlan** command multiple times, the trunk port carries the set of VLANs specified by *vlan-id-list* in each execution.

The **port trunk permit vlan all** command can be ineffective to voice VLANs. If you are prompted with a configuration error message when using this command, use the **display this** command to view the execution result.

On a trunk port, only traffic of the PVID can pass through untagged.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

On GVRP-enabled trunk ports, you must configure the **port trunk permit vlan all** command to make sure that the traffic of all dynamically registered VLANs can pass through. To prevent unauthorized VLAN users from accessing restricted resources through a GVRP-disabled port, do not use the **port trunk permit vlan all** command on the port.

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

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
Please wait........... Done.
```

# Assign the trunk Layer 2 aggregate interface Bridge-Aggregation 1 to VLAN 2.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type trunk
[Sysname-Bridge-Aggregation1] port trunk permit vlan 2
 Please wait... Done.
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
```

The output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are the member ports of the aggregation group corresponding to Bridge-Aggregation 1.

port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

View

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

Default level

2: System level

Parameters

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

Description

Use **port trunk pvid** to configure the PVID for the trunk port.

Use **undo port trunk pvid** to restore the default.

By default, the PVID of a trunk port is VLAN 1.

You can use a nonexistent VLAN as the PVID for a trunk port. If you use the **undo vlan** command to remove the PVID of a hybrid port, it does not affect the setting of the PVID on the port.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

The local and remote trunk ports must use the same PVID for the traffic of the PVID to be transmitted properly.

You must use the **port trunk permit vlan** command to configure the trunk port to allow and forward packets from the PVID.

Related commands: **port link-type** and **port trunk permit vlan**.

Examples

# Configure VLAN 100 as the PVID of the trunk port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

# Configure VLAN 100 as the PVID of the trunk Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type trunk
[Sysname-Bridge-Aggregation1] port trunk pvid vlan 100
```

MAC-based VLAN configuration commands

display mac-vlan

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* | **static** | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all the MAC address-to-VLAN entries.

dynamic: Displays dynamically configured MAC address-to-VLAN entries.

mac-address *mac-address*: Displays the MAC address-to-VLAN entry containing the specified MAC address.

static: Displays the statically configured MAC address-to-VLAN entries.

vlan *vlan-id*: Displays the MAC address-to-VLAN entries associated with the specified VLAN.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-vlan** to display the specified MAC address-to-VLAN entries.

Examples

# Display all the MAC address-to-VLAN entries.

```
<Sysname> display mac-vlan all
The following MAC-VLAN address exist:
S: Static   D: Dynamic
MAC ADDR           MASK                    VLAN ID   PRIO    STATE
--------------------------------------------------------------------
0008-0001-0000     FFFF-FFFF-FFFF          5         3       S
0002-0001-0000     FFFF-FFFF-FFFF          5         3       S&D

Total MAC VLAN address count:2
```

Table 36 Command output

Field	Description
S: Static	The character **S** stands for the MAC address-to-VLAN entries that are configured statically.
D: Dynamic	The character **D** stands for the MAC address-to-VLAN entries that are configured dynamically.
MAC ADDR	MAC address of a MAC address-to-VLAN entry.
MASK	Mask of the MAC address of a MAC address-to-VLAN entry.
VLAN ID	VLAN ID of a MAC address-to-VLAN entry.
PRIO	802.1p priority corresponding to the MAC address of a MAC address-to-VLAN entry
STATE	State of a MAC address-to-VLAN entry: • **S**—The MAC address-to-VLAN entry is configured statically. • **D**—The MAC address-to-VLAN entry is configured automatically through the authentication server. • **S&D**—The MAC address-to-VLAN entry is configured both statically and dynamically.

display mac-vlan interface

Syntax

display mac-vlan interface [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-vlan interface** to display all the ports with MAC-based VLAN enabled.

Related commands: **mac-vlan enable**.

Examples

# Display all the interfaces with MAC-based VLAN enabled.

```
<Sysname> display mac-vlan interface
MAC VLAN is enabled on following ports:
---------------------------------------
GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

mac-vlan enable

Syntax

mac-vlan enable

undo mac-vlan enable

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

None

Description

Use **mac-vlan enable** to enable the MAC-based VLAN feature on a port.

Use **undo mac-vlan enable** to disable the MAC-based VLAN feature on a port.

By default, the MAC-based VLAN feature is disabled on a port.

Examples

# Enable the MAC-based VLAN feature on GigabitEthernet 1/0/1.

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

mac-vlan mac-address

Syntax

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

undo mac-vlan { **all** | **mac-address** *mac-address* | **vlan** *vlan-id* }

View

System view

Default level

2: System level

Parameters

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

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

priority *pri*: Specifies the 802.1p priority value corresponding to the specified MAC address. The *pri* argument ranges from 0 to 7.

all: Removes all the static MAC address-to-VLAN entries.

Description

Use **mac-vlan mac-address** to associate the specified VLAN and priority value with the specified MAC addresses.

Use **undo mac-vlan** to remove the association.

The MAC-to-VLAN entry maintained by the device describes the relationship between a MAC address and a VLAN, and a priority value. The system adds/removes MAC address-to-VLAN entries to/from the table according to the configuration.

Examples

# Associate a single MAC address 0-1-1 with VLAN 100 and 802.1p priority 7.

```
<Sysname> system-view
[Sysname] mac-vlan mac-address 0-1-1 vlan 100 priority 7
```

mac-vlan trigger enable

Syntax

mac-vlan trigger enable

undo mac-vlan trigger enable

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

None

Description

Use **mac-vlan trigger enable** to enable dynamic MAC-based VLAN assignment. The port configured with this command will be dynamically assigned to VLANs based on the source MAC addresses of the received packets.

Use **undo mac-vlan trigger enable** to restore the default.

By default, dynamic MAC-based VLAN assignment is not enabled.

After receiving a packet with an unknown source MAC address, a port submits the packet to the CPU.

If the source MAC address matches a MAC address-to-VLAN entry maintained by the device, the device dynamically learns the source MAC address and assigns the receiving port to the corresponding VLAN. Then, subsequent packets with this source MAC address can be directly forwarded through the port.

If the MAC address does not match any MAC address-to-VLAN entry, the device will not dynamically learn the MAC address and assign the receiving port to the corresponding VLAN.

Examples

# Enable dynamic MAC-based VLAN assignment on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-vlan trigger enable
```

port pvid disable

Syntax

port pvid disable

undo port pvid disable

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

None

Description

Use **port pvid disable** to disable the PVID of the port from forwarding packets whose source MAC addresses do not match any MAC address-to-VLAN entry.

Use **undo port pvid disable** to restore the default.

By default, when a port receives a packet with an unknown source MAC address that does not match any MAC address-to-VLAN entry, it forwards the packet in its PVID.

Examples

# Disable the PVID of GigabitEthernet 1/0/1 from forwarding packets whose source MAC addresses do not match any MAC address-to-VLAN entry.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port pvid disable
```

vlan precedence

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

View

Layer 2 Ethernet port view, port group view

Default level

2: System level

Parameters

mac-vlan: Matches VLANs based on MAC addresses preferentially.

ip-subnet-vlan: Matches VLANs based on IP subnet settings preferentially.

Description

Use **vlan precedence** to set the order of VLAN matching.

Use **undo vlan precedence** to restore the default.

By default, VLANs are matched based on MAC addresses preferentially.

This command only applies to VLANs based on a single MAC address and IP subnet-based VLANs.

If both the MAC-based VLAN function and the IP subnet-based VLAN function are created on a port, MAC address-to-VLAN entries are matched preferentially, and the remaining VLAN entries (VLAN entries based on a single MAC address and IP subnet-based VLANs) are matched as configured by the **vlan precedence** command.

Examples

# Configure matching VLANs based on MAC addresses preferentially on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

Protocol-based VLAN configuration commands

display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface-type interface-number1: Specifies an interface by its type and number.

interface-type interface-number1 **to** *interface-type interface-number2*: Specifies an interface range.

all: Displays information about protocol-based VLANs on all ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display protocol-vlan interface** to display information about protocol-based VLANs for the specified ports.

Examples

# Display protocol-based VLAN information on GigabitEthernet 1/0/1.

```
[Sysname] display protocol-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
   VLAN ID   Protocol Index      Protocol Type
 ======================================================
       2          0               ipv6
       3          0               ipv4
```

Table 37 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN bound to the port
Protocol Index	Protocol template index
Protocol Type	Protocol type specified by the protocol template

display protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

vlan-id1: Specifies a protocol-based VLAN ID, in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Displays protocol-based VLAN information of a VLAN that is in the range of *vlan-id1* to *vlan-id2*. The *vlan-id2* argument specifies a protocol-based VLAN ID, in the range of 1 to 4094, but you must make sure that its value is greater than or equal to that of *vlan-id1*.

all: Displays information about all protocol-based VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display protocol-vlan vlan** to display the protocols and protocol indexes configured on the specified VLANs.

Related commands: **display vlan**.

Examples

# Display the protocols and protocol indexes configured on all protocol-based-VLANs.

```
<Sysname> display protocol-vlan vlan all
 VLAN ID:2
    Protocol Index      Protocol Type
 ======================================================
          0              ipv4
          3              ipv6
 VLAN ID:3
    Protocol Index      Protocol Type
 ======================================================
          0              ipv4
          1              ipv6
```

Table 38 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN bound to the port
Protocol Index	Protocol template index
Protocol Type	Protocol type specified by the protocol template

port hybrid protocol-vlan

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo port hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

View

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

Default level

2: System level

Parameters

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

protocol-index: Specifies a protocol index. The value can be specified by the users or assigned by the system automatically when the protocol-based VLAN is created. You can use the **display protocol-vlan vlan all** command to display the protocol indexes. The *protocol-index* argument ranges from 0 to 15.

to *protocol-end*: Specifies the end protocol index. The *protocol-end* argument must be greater than or equal to the beginning protocol index. The *protocol-end* argument is in the range of 0 to 15.

all: Specifies all protocols bound to *vlan-id*.

Description

Use **port hybrid protocol-vlan** to associate the hybrid ports with a protocol-based VLAN.

Use **undo port hybrid protocol-vlan** to remove the association.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

Before you use this command, make the following configurations:

- Create a VLAN and associate it with specified protocols.
- Configure the link type as hybrid.
- Configure the port to allow the protocol-based VLAN to pass through.

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

Examples

# Associate the hybrid port GigabitEthernet 1/0/1 with protocol 0 (IPv4) in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan ipv4
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
 Please wait... Done
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 0
```

# Associate the hybrid Layer 2 aggregate interface Bridge-Aggregation 1 with protocol 0 in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan ipv4
[Sysname-vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 0
```

The output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are the member ports of the aggregation group corresponding to Bridge-Aggregation 1.

protocol-vlan

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

View

VLAN view

Default level

2: System level

Parameters

at: Specifies the AppleTalk based VLAN.

ipv4: Specifies the IPv4 based VLAN.

ipv6: Specifies the IPv6 based VLAN.

ipx: Specifies the IPX based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** are encapsulation formats for IPX.

mode: Configures a user-defined protocol template for the VLAN, which could also have the following encapsulation formats: **ethernetii**, **llc**, and **snap**.

ethernetii etype *etype-id*: Matches Ethernet II encapsulation format and the corresponding protocol type values. The *etype-id* argument is the protocol type ID of inbound packets, in the range of 0x0600 to 0xFFFF (excluding 0x0800, 0x809B, 0x8137, and 0x86DD).

llc: Matches the **llc** encapsulation format.

dsap *dsap-id*: Specifies the destination service access point, in the range of 0x00 to 0xFF.

ssap *ssap-id*: Specifies the source service access point, in the range of 0x00 to 0xFF.

snap etype *etype-id*: Matches SNAP encapsulation format and the corresponding protocol type values. The *etype-id* argument is the Ethernet type of inbound packets, in the range of 0x0600 to 0xFFFF (excluding 0x8137).

protocol-index: Specifies a protocol template index, in the range of 0 to 15. The system will automatically assign an index if this parameter is not specified.

to *protocol-end*: Specifies the end protocol index, in the range of 0 to 15. The *protocol-end* argument must be greater than or equal to the *protocol-index* argument.

all: Removes all the protocols bound to the VLAN.

Description

Use **protocol-vlan** to configure the VLAN as a protocol based VLAN and configure the protocol template for the VLAN.

Use **undo protocol-vlan** to remove the configured protocol template.

By default, no VLAN is bound to any protocol template.

When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **ethernetii etype** *etype-id* to 0x0800, 0x809B, 0x8137, or 0x86DD. Otherwise, the encapsulation format of the matching packets will be the same as that of the IPv4, AppleTalk, IPX, and IPv6 packets, respectively.

Do not configure both the *dsap-id* and *ssap-id* arguments in the **protocol-vlan** command as 0xE0 or 0xFF when you configure the user-defined template for **llc** encapsulation. Otherwise, the encapsulation format of the matching packets will be the same as that of the **ipx llc** or **ipx raw** packets, respectively. When either of the *dsap-id* and *ssap-id* arguments is configured, the system assigns 0XAA to the other argument.

When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **snap etype** *etype-id* to 0x8137. Otherwise, the template format will be the same as that of the IPX protocol. You can set *etype-id* to 0x0800, 0x809B, or 0x86DD, corresponding to IPv4, AppleTalk, and IPv6, respectively.

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

Examples

△ CAUTION:

IP uses ARP for address resolution in Ethernet. To prevent communication failure, configure the IP and ARP templates in the same VLAN and associate them with the same port.

# Configure VLAN 3 as an IPv4 based VLAN.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan ipv4
```

# Create an ARP protocol template for VLAN 3 (ARP code is 0x0806) to make VLAN 3 transmit ARP packets.

- To use Ethernet encapsulation, use this command:

```
[Sysname-vlan3] protocol-vlan mode ethernetii etype 0806
```

- To use 802.3 encapsulation, use this command:

```
[Sysname-vlan3] protocol-vlan mode snap etype 0806
```

IP subnet-based VLAN configuration commands

display ip-subnet-vlan interface

Syntax

display ip-subnet-vlan interface { *interface-list* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

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

all: Displays IP subnet information about all the ports with IP subnet-based VLAN configured.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip-subnet-vlan interface** to display IP subnet-based VLANs and IP subnet indexes on the specified ports.

Examples

# Display IP subnet-based VLANs and IP subnet indexes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] display ip-subnet-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet-Index    IP ADDRESS         NET MASK
  =======================================================
     3           0             192.168.1.0    255.255.255.0
```

Table 39 Command output

Field	Description
Subnet-Index	Index of the IP subnet
IP ADDRESS	IP address of the subnet (either an IP address or a network address)
NET MASK	Mask of the IP subnet

display ip-subnet-vlan vlan

Syntax

display ip-subnet-vlan vlan { *vlan-id* [**to** *vlan-id*] | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

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

to: Specifies a VLAN ID range. The argument after this keyword must be greater than or equal to the one before this keyword.

all: Specifies all the VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip-subnet-vlan vlan** to display the IP subnet information and IP subnet indexes on the specified VLANs.

Related commands: **display vlan**.

Examples

# Display the IP subnet information and IP subnet indexes for all VLANs.

```
<Sysname> display ip-subnet-vlan vlan all
VLAN ID:  3
 Subnet Index      IP Address      Subnet Mask
 ====================================================
       0          192.168.1.0    255.255.255.0
```

Table 40 Command output

Field	Description
Subnet Index	IP subnet index.
IP Address	IP address of the subnet. It can be an IP address or a network address.
Subnet Mask	Mask of the IP subnet.

ip-subnet-vlan

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

View

VLAN view

Default level

2: System level

Parameters

ip-subnet-index: Specifies a beginning IP subnet index, in the range of 0 to 11. The value can be configured by users, or automatically numbered by the system, based on the order in which the IP subnets or IP addresses are associated with the VLAN.

ip *ip-address* [*mask*]: Specifies the source IP address or network address based on which the subnet-based VLANs are classified, in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

to: Specifies an IP subnet index range.

ip-subnet-end: Specifies an end IP subnet index, in the range of 0 to 11. The value must be greater than or equal to the beginning IP subnet index.

all: Removes all the associations between VLANs and IP subnets or IP addresses.

Description

Use **ip-subnet-vlan** to associate the VLAN with a specified IP subnet or IP address.

Use **undo ip-subnet-vlan** to remove the association.

The IP subnet or IP address cannot be a multicast network segment or a multicast address.

Related commands: **display ip-subnet-vlan vlan**.

Examples

# Configure VLAN 3 as an IP subnet-based VLAN and associate it with the 192.168.1.0/24 network segment.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

port hybrid ip-subnet-vlan

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

View

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

Default level

2: System level

Parameters

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

all: Specifies all VLANs.

Description

Use **port hybrid ip-subnet-vlan** to associate the Ethernet port with the specified IP subnet-based VLAN.

Use **undo port hybrid ip-subnet-vlan** to remove the association.

On an Ethernet port associated with an IP subnet-based VLAN, if the source IP address of a received untagged packet belongs to the corresponding IP subnet, the port tags the packet with the corresponding VLAN tag.

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

The configuration made in port group view applies to all ports in the port group.

The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports.

- If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
- If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port.

Only hybrid ports support this feature. Before you use this command, assign the port to the IP subnet-based VLAN you want to associate with.

Related commands: **display ip-subnet-vlan interface**.

Examples

# Associate GigabitEthernet 1/0/1 with the IP subnet-based VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
 Please wait... Done.
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

# Associate the hybrid Layer 2 aggregate interface Bridge-Aggregation 1 with the IP subnet-based VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
 Please wait... Done
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

The output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are the member ports of the aggregation group corresponding to Bridge-Aggregation 1.

Isolate-user-VLAN configuration commands

display isolate-user-vlan

Syntax

display isolate-user-vlan [*isolate-user-vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

isolate-user-vlan-id: Specifies an isolate-user-VLAN ID, in the range of 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isolate-user-vlan** to display the mapping between an isolate-user-VLAN and secondary VLANs.

Related commands: **isolate-user-vlan** and **isolate-user-vlan enable**.

Examples

# Display the mapping between an isolate-user-VLAN and secondary VLANs.

```
<Sysname> display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 2
 Secondary VLAN ID : 3 4

 VLAN ID: 2
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 IPv6 global unicast address(es):
    2001::1, subnet is 2001::/64 [TENTATIVE]
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports: none
```

```
Untagged Ports:
   GigabitEthernet1/0/2           GigabitEthernet1/0/3           GigabitEthernet1/0/4

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/2            GigabitEthernet1/0/3

VLAN ID: 4
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged   Ports: none
Untagged Ports:
  GigabitEthernet1/0/2            GigabitEthernet1/0/4
```

Table 41 Command output

Field	Description
Isolate-user-VLAN VLAN ID	Isolate-user-VLAN ID.
Secondary VLAN ID	Secondary VLAN ID.
VLAN Type	VLAN type (static or dynamic).
Isolate-user-VLAN type	Current VLAN type (isolate-user-VLAN or secondary VLAN).
Route Interface	Indicates whether a VLAN interface is configured for the VLAN.
IPv4 address	IPv4 address of the VLAN interface (available only when an IPv4 address is configured for the VLAN interface).
IPv4 subnet mask	Subnet mask of the IPv4 address (available only when an IPv4 address is configured for the VLAN interface).
IPv6 global unicast address(es)	Global unicast IPv6 address of the VLAN interface (available only when an IPv6 address is configured for the VLAN interface).
Tagged Ports	Ports through which packets of this VLAN are sent tagged.
Untagged Ports	Ports through which packets of this VLAN are sent untagged.

isolate-user-vlan

Syntax

isolate-user-vlan *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

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

View

System view

Default level

2: System level

Parameters

isolate-user-vlan-id: Specifies an isolate-user-VLAN ID, in the range of 1 to 4094. Do not specify VLAN 1 for this argument.

secondary *secondary-vlan-id* [**to** *secondary-vlan-id*]: Specifies a secondary VLAN ID or a secondary VLAN ID range. The *secondary-vlan-id* argument is a secondary VLAN ID, in the range of 1 to 4094. Do not specify VLAN 1 for this argument.

Description

Use **isolate-user-vlan** to associate an isolate-user-VLAN with the specified secondary VLANs.

Use **undo isolate-user-vlan** to remove the association.

By default, an isolate-user-VLAN is not associated with any secondary VLAN. .

The **undo isolate-user-vlan** command without the **secondary** *secondary-vlan-id* parameter specified removes the association between the specified isolate-user-VLAN and all its secondary VLANs.

The **undo isolate-user-vlan** command with the **secondary** *secondary-vlan-id* parameter specified only removes the association between the specified isolate-user-VLAN and the specified secondary VLANs.

Do not configure the default VLAN (VLAN 1) as a secondary VLAN or isolate-user-VLAN.

Related commands: **display isolate-user-vlan**.

Examples

# Associate isolate-user-VLAN 2 with secondary VLANs VLAN 3 and VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port gigabitethernet 1/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/3
[Sysname-vlan3] vlan 4
[Sysname-vlan4] port gigabitethernet 1/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
```

isolate-user-vlan enable

Syntax

isolate-user-vlan enable

undo isolate-user-vlan enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **isolate-user-vlan enable** to configure the VLAN as an isolate-user-VLAN.

Use **undo isolate-user-vlan enable** to remove the isolate-user-VLAN configuration for the VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including the one connected to the upstream device.

Do not configure the default VLAN (VLAN 1) as a secondary VLAN or isolate-user-VLAN.

Related commands: **display isolate-user-vlan**.

Examples

# Configure VLAN 5 as an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```

isolated-vlan enable

Syntax

isolated-vlan enable

undo isolated-vlan enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **isolated-vlan enable** to configure Layer 2 isolation between ports in the same secondary VLAN.

Use **undo isolated-vlan enable** to restore the default.

By default, ports in the same secondary VLAN can communicate at Layer 2.

You cannot configure Layer 2 isolation between ports in an isolate-user-VLAN.

Layer 2 isolation configured with the **isolated-vlan enable** command takes effect only when the isolate-user-VLAN type of each port in the secondary VLAN is configured as **host** and the secondary VLAN is associated with an isolate-user-VLAN.

After you configure the **isolated-vlan enable** command in VLAN view, you cannot assign any port in the VLAN to an isolation group.

Layer 2 isolation configured with the **isolated-vlan enable** command takes effect only after the secondary VLAN is associated with an isolate-user-VLAN.

Related commands: **isolate-user-vlan**.

Examples

# Configure Layer 2 isolation between ports in secondary VLAN 4, where GigabitEthernet 1/0/1 is the uplink port and GigabitEthernet 1/0/2 is the downlink port.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] quit
[Sysname] vlan 4
[Sysname-vlan4] isolated-vlan enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 untagged
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type hybrid
[Sysname-GigabitEthernet1/0/2] port hybrid vlan 2 4 untagged
[Sysname-GigabitEthernet1/0/2] port hybrid pvid vlan 4
[Sysname-GigabitEthernet1/0/2] port isolate-user-vlan host
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] isolate-user-vlan 2 secondary 4
```

port isolate-user-vlan promiscuous

Syntax

port isolate-user-vlan *vlan-id* **promiscuous**

undo port isolate-user-vlan

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

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

Description

Use **port isolate-user-vlan promiscuous** command to configure a port to operate in promiscuous mode in a VLAN and assign the port to the VLAN. If the VLAN is an isolate-user-VLAN, this command simultaneously assigns the port to the secondary VLANs associated with the isolate-user-VLAN.

Use **undo port isolate-user-vlan** to cancel the promiscuous operating mode of a port.

By default, a port does not operate in promiscuous mode in a VLAN.

Before configure a port to operate in promiscuous mode in a VLAN, make sure that the VLAN has been created.

When the device executes the **port isolate-user-vlan** *vlan-id* **promiscuous** command, the following guidelines apply:

- If the port is an access port:
    - If the specified VLAN is an isolate-user-VLAN that has not been associated with any secondary VLAN, the system automatically assigns the port to the VLAN as an access port.
    - If the specified VLAN is an isolate-user-VLAN associated with secondary VLANs, the system changes the link type of the port to hybrid, sets the isolate-user-VLAN as the PVID of the port, and assigns the port to the associated secondary VLANs.
- If the port is a hybrid port, the system automatically assigns the port to the isolate-user-VLAN and its associated secondary VLANs (if the isolate-user-VLAN has been associated with secondary VLANs) as an untagged member (if the port has been assigned to a secondary VLAN as a tagged member, the tagged member attribute is not changed), and keeps the PVID of the port. You can manually set a proper PVID for the port.
- If the port is a trunk port, the system automatically assign the port to the isolate-user-VLAN and its associated secondary VLANs, and keeps the PVID. You can manually set a proper PVID for the port.

When you use the **port isolate-user-vlan** *vlan-id* **promiscuous** command on a port that operates in promiscuous mode, the device automatically executes the **undo port isolate-user-vlan** command to cancel the promiscuous mode of the port first.

The **undo port isolate-user-vlan** command does not remove a port from secondary VLANs or change its link type and PVID, does not remove an access port from the specific VLAN, but removes a trunk or hybrid port from the specific VLAN.

You can configure the **port isolate-user-vlan** *vlan-id* **promiscuous** command and the **isolate-user-vlan enable** command in any order.

Examples

# Configure access port GigabitEthernet 1/0/1 to operate in promiscuous mode in isolate-user-VLAN 2, which is associated with secondary VLAN 20, and then cancel the configuration.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 2 promiscuous
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 2
```

```
#
return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 20 untagged
 port hybrid pvid vlan 2
#
return
```

# Assign access port GigabitEthernet 1/0/1 to VLAN 10, which is not an isolate-user-VLAN, configure the port to operate in promiscuous mode in VLAN 10, and then cancel the configuration.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 10 promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 10 promiscuous
 port access vlan 10
#
return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
return
```

port isolate-user-vlan host

Syntax

port isolate-user-vlan host

undo port isolate-user-vlan

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **port isolate-user-vlan host** to configure a port to operate in host mode. If the port is assigned to a secondary VLAN, the command also simultaneously assigns the port to the isolate-user-VLAN that is associated with the secondary VLAN.

Use **undo port isolate-user-vlan** to cancel the host operating mode of a port.

By default, a port does not operate in host mode.

When you execute the **port isolate-user-vlan host** command for the port in a secondary VLAN, the following guidelines apply:

- If the port is an access port, the system changes the link type of the port to hybrid, assigns the port to the associated isolate-user-VLAN as an untagged member, and configures the secondary VLAN as the PVID of the port.
- If the port is a hybrid port, the system automatically assigns the port to the associated isolate-user-VLAN as an untagged member (if the port has been assigned to the isolate-user-VLAN as a tagged member, the tagged member attribute is not changed), and keeps the PVID of the port. You can manually set a proper PVID for the port.
- If the port is a trunk port, the system automatically assigns the port to the associated isolate-user-VLAN, and keeps the PVID. You can manually set a proper PVID for the port.

You can configure the **port isolate-user-vlan host** command before or after assigning the port to a secondary VLAN.

Examples

# Configure access port GigabitEthernet 1/0/1 to operate in host mode and assign the port to secondary VLAN 20, which is associated with isolate-user-VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan host
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan host
#
return
[Sysname-GigabitEthernet1/0/1] port access vlan 20
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan host
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 20
#
return
```

Voice VLAN configuration commands

display voice vlan oui

Syntax

display voice vlan oui [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display voice vlan oui** to display the supported organizationally unique identifier (OUI) addresses, the OUI address masks, and the description strings.

OUI addresses are used to determine whether a received packet is a voice packet. They are the results of the AND operation of the two arguments *mac-address* and *oui-mask* in the **voice vlan mac-address** command.

Related commands: **voice vlan mac-address**.

Examples

# Display the supported OUI addresses, and their masks and descriptions.

```
<Sysname> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Table 42 Command output

Field	Description
Oui Address	OUI addresses supported

Field	Description
Mask	Masks of the OUI addresses supported
Description	Description strings of the OUI addresses supported

display voice vlan state

Syntax

display voice vlan state [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display voice vlan state** to display voice VLAN configuration.

Related commands: **voice vlan enable**, **voice vlan qos**, and **voice vlan qos trust**.

Examples

# Display voice VLAN configurations.

```
<Sysname> display voice vlan state
Maximum of Voice VLANs: 8
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE        COS        DSCP
 --------------------------------------------------------------------
 GigabitEthernet1/0/11       111         AUTO        6          46
```

Table 43 Command output

Field	Description
Voice VLAN system capacity	Maximum number of voice VLANs supported by the system.
Current Voice VLAN Count	Number of existing voice VLANs.

Field	Description
Voice VLAN security mode	Security mode of the voice VLAN: • **Security**—Security mode. • **Normal**—Normal mode.
Voice VLAN aging time	Aging time of the voice VLAN.
Current voice vlan enabled port and its mode	Voice VLAN-enabled port and its voice VLAN assignment mode.
PORT	Voice VLAN-enabled port name.
VLAN	ID of the voice VLAN enabled on the port.
MODE	Voice VLAN assignment mode of the port, manual or automatic.
COS	Class of Service.
DSCP	Differentiated Services Codepoint Priority.

voice vlan aging

Syntax

voice vlan aging *minutes*

undo voice vlan aging

View

System view

Default level

2: System level

Parameters

minutes: Sets the voice VLAN aging time, in the range of 5 to 43200 minutes.

Description

Use **voice vlan aging** to configure the voice VLAN aging time.

Use **undo voice vlan aging** to restore the default.

By default, the voice VLAN aging time is 1440 minutes.

When a port in automatic voice VLAN assignment mode receives a voice packet, the system decides whether to assign the port to the voice VLAN based on the source MAC address of the voice packet. Upon assigning the port to the voice VLAN, the system starts the aging timer. If no voice packets are received on the port until the aging time expires, the system automatically removes the port from the voice VLAN. This aging time applies only to the ports in automatic voice VLAN assignment mode.

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

Examples

# Configure the voice VLAN aging time as 100 minutes.

```
<Sysname> system-view
[Sysname] voice vlan aging 100
```

voice vlan enable

Syntax

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

undo voice vlan [*vlan-id*] **enable**

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN ID, in the range of 2 to 4096.

Description

Use **voice vlan enable** to enable the voice VLAN feature and configure a VLAN as the voice VLAN for the Ethernet port.

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

By default, the voice VLAN feature is disabled on ports.

Enable the voice VLAN feature on a hybrid or trunk port operating in automatic voice VLAN assignment mode, but not on an access port operating in automatic voice VLAN assignment mode.

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan 2 enable
```

voice vlan mac-address

Syntax

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

undo voice vlan mac-address *oui*

View

System view

Default level

2: System level

Parameters

mac-address: Specifies a source MAC address of voice traffic, in the format of H-H-H. For example, 1234-1234-1234.

mask *oui-mask*: Specifies the valid length of the OUI address by a mask in the format of H-H-H, formed by consecutive 1s and 0s. For example, FFFF-0000-0000. To filter the voice device of a specific vendor, set the mask to FFFF-FF00-0000.

description *text*: Specifies a string of 1 to 30 case-sensitive characters that describes the OUI address.

oui: Specifies the OUI address you want to remove, in the format of H-H-H. For example, 1234-1200-0000. An OUI address is the logic AND result of *mac-address* and *oui-mask*. An OUI address cannot be a broadcast address, a multicast address, or an all-zero address.

Description

Use **voice vlan mac-address** to allow packets carrying the specified OUI address to pass through.

Use **undo voice vlan mac-address** to prohibit packets carrying the specified OUI address from passing through.

Use **display voice vlan oui** to display the OUI addresses supported.

By default, the system is configured with the default OUI addresses. You can remove the default OUI addresses and then add recognizable OUI addresses manually.

The Switch Series supports up to 16 OUI addresses.

Table 44 Default OUI addresses

Number	OUI address	Vendor
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	00D0-1E00-0000	Pingtel phone
5	0060-B900-0000	Philips/NEC phone
6	00E0-7500-0000	Polycom phone
7	00E0-BB00-0000	3Com phone

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

Examples

# Add a recognizable OUI address 1234-1200-0000 by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000, and configure its description string as **PhoneA**.

```
<Sysname> system-view
[Sysname] voice vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

voice vlan mode auto

Syntax

voice vlan mode auto

undo voice vlan mode auto

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **voice vlan mode auto** to configure the port to operate in automatic voice VLAN assignment mode.

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

By default, a port operates in automatic voice VLAN assignment mode.

The voice VLAN modes of different ports are independent of one another.

To make voice VLAN take effect on a port which is enabled with voice VLAN and operates in manual voice VLAN assignment mode, assign the port to the voice VLAN manually.

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice vlan mode auto
```

voice vlan qos

Syntax

voice vlan qos *cos-value dscp-value*

undo voice vlan qos

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

cos-value: Sets the CoS precedence value for voice VLAN traffic. The default value is 6.

dscp-value: Sets the DSCP value for voice VLAN traffic. The default value is 46.

Description

Use **voice vlan qos** to configure the interface to modify the CoS and DSCP values marked for incoming traffic of the voice VLAN into specified values.

Use **undo voice vlan qos** to restore the default.

By default, an interface modifies the CoS value and the DSCP value marked for voice VLAN traffic into 6 and 46, respectively.

Configure the QoS priority settings for voice VLAN traffic on an interface before you enable voice VLAN on the interface. If the configuration order is reversed, the priority settings will fail.

The **voice vlan qos** command and the **voice vlan qos trust** command can overwrite each other. When you execute the two commands on a port multiple times, the most recent one takes effect.

Related commands: **voice vlan qos trust**.

Examples

# Configure interface GigabitEthernet 1/0/1 to modify the CoS value and the DSCP value marked for voice VLAN packets into 5 and 45, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan qos 5 45
```

voice vlan qos trust

Syntax

voice vlan qos trust

undo voice vlan qos

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **voice vlan qos trust** to configure the interface to trust the priority settings carried in incoming voice traffic. With this command configured, an interface keeps the CoS and DSCP values marked for incoming voice traffic unchanged.

Use **undo voice vlan qos** to restore the default.

By default, an interface modifies the CoS value and the DSCP value marked for voice VLAN traffic into 6 and 46, respectively.

Configure the QoS priority trust mode for voice VLAN traffic on an interface before enabling voice VLAN on the interface. If the configuration order is reversed, your priority trust setting will fail.

The **voice vlan qos** command and the **voice vlan qos trust** command can overwrite each other. After you execute the two commands on a port multiple times, the one that was last executed takes effect.

Related commands: **voice vlan qos**.

Examples

# Configure interface GigabitEthernet 1/0/1 to trust the priority settings carried in incoming voice VLAN traffic.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan qos trust
```

voice vlan security enable

Syntax

voice vlan security enable

undo voice vlan security enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **voice vlan security enable** to enable the voice VLAN security mode.

Use **undo voice vlan security enable** to disable the voice VLAN security mode.

By default, the voice VLAN security mode is enabled.

When you enable the security mode for a voice VLAN, only voice traffic can be transmitted in the voice VLAN.

The device matches the source MAC addresses of the packets against the supported OUI addresses to determine whether they are voice traffic and filters all non-voice traffic, guaranteeing high priority and high quality for voice traffic.

When a voice VLAN operates in common mode, other data traffic is also transmitted in the voice VLAN.

Examples

# Disable voice VLAN security mode.

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

GVRP configuration commands

display garp statistics

Syntax

display garp statistics [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Displays the GARP statistics of one or multiple ports. You can specify up to 10 port lists.

- You can specify a single port in the form of *interface-type interface-number*.
- You can specify a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end port number specified by *interface-number2* must be greater than the start port number specified by *interface-number1*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display garp statistics** to display the GARP statistics of the specified ports. If no ports are specified, this command displays the GARP statistics for all ports.

This command displays the statistics about GVRP PDUs received, transmitted, and dropped on GVRP-enabled ports. When the system is restarted or after you perform the **reset garp statistics** command, the existing packet statistics are cleared and the system starts to collect new GARP statistics. With the statistics, you can judge whether a GVRP-enabled port is operating properly.

- If the number of received and transmitted GVRP PDUs on the port is the same as the remote port, it indicates that the two ends are transmitting and receiving GVRP PDUs properly and no registration information is lost.
- If the port drops GVRP PDUs, you should check its registration mode. GVRP PDUs are likely to be dropped if the registration mode is fixed or forbidden, because dynamic VLANs cannot be registered in these two modes.

Related commands: **reset garp statistics**.

Examples

# Display GARP statistics on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> display garp statistics interface gigabitethernet 1/0/1 to gigabitethernet 1/0/2

         GARP statistics on port GigabitEthernet1/0/1

         Number of GVRP Frames Received          : 5
         Number of GVRP Frames Transmitted       : 2
         Number of Frames Discarded              : 1

         GARP statistics on port GigabitEthernet1/0/2

         Number of GVRP Frames Received          : 3
         Number of GVRP Frames Transmitted       : 4
         Number of Frames Discarded              : 2
```

display garp timer

Syntax

display garp timer [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Displays the GARP timer settings of one or multiple ports. You can specify up to 10 port lists.

- You can specify a single port in the form of *interface-type interface-number*.
- You can specify a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end port number specified by *interface-number2* must be greater than the start port number specified by *interface-number1*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display garp timer** to display GARP timers on specific ports. If no ports are specified, this command displays the GARP timers on all ports.

Related commands: **garp timer hold**, **garp timer join**, **garp timer leave**, and **garp timer leaveall**.

Examples

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

```
<Sysname> display garp timer interface gigabitethernet 1/0/1
         GARP timers on port GigabitEthernet1/0/1
```

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

display gvrp local-vlan

Syntax

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

View

Any view

Default level

0: Visit level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display gvrp local-vlan** to display the local VLAN information maintained by GVRP on the specified port.

Examples

# Display the local VLAN information maintained by GVRP on GigabitEthernet 1/0/1.

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

display gvrp state

Syntax

display gvrp state interface *interface-type interface-number* **vlan** *vlan-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

0: Visit level

Parameters

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

vlan *vlan-id*: Specifies a VLAN ID, ranging from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display gvrp state** to display GVRP state machines in a specified VLAN on a port.

Examples

# Display GVRP state machines in VLAN 2 on port GigabitEthernet 1/0/1.

```
<Sysname> display gvrp state interface gigabitethernet 1/0/1 vlan 2
        GVRP state of VLAN 2 on port GigabitEthernet1/0/1

                 Applicant state machine      : VP
                 Registrar state machine      : MTR
```

Table 45 Command output

Field	Description
GVRP state of VLAN 2 on port GigabitEthernet1/0/1	Information about the GVRP state machines in VLAN 2 on port GigabitEthernet 1/0/1.
Applicant state machine	Applicant state machine handles attribute declarations. Its state can be VA, AA, QA, LA, VP, AP, QP, VO, AO, QO, LO, VON, AON, and QON. Each state consists of two or three letters with the following meanings: • The first letter indicates the state: V for Very anxious, A for Anxious, Q for Quiet, and L for Leaving. • The second letter indicates the membership state: A for Active member, P for Passive member, and O for Observer. • The third letter N (if any) stands for Non-participant. For example, VP indicates "Very anxious, Passive member".

Field	Description
Registrar state machine	Registrar state machine records the registration of attributes declared by other participants. Its state can be INN, LV, L3, L2, L1, MT, INR, LVR, L3R, L2R, L1R, MTR, INF, LVF, L3F, L2F, L1F, and MTF. Each state consists of two or three letters or numbers with the following meanings: • The first two letters or numbers indicate the state: IN stands for In; LV, L3, L2, and L1 all stand for Leaving, and L3, L2, L1 are three sub-states of LV; MT stands for Empty • The third letter indicates the registration mode: N (if any) for Normal registration, R for Registration fixed, and F for Registration forbidden. For example, MTR stands for "Empty, Registration fixed", indicating the fixed registration mode in Empty state.

display gvrp statistics

Syntax

display gvrp statistics [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Displays the GVRP statistics of one or multiple Ethernet ports.

You can provide up to 10 Ethernet port lists, specified in the following ways:

- As an individual port in the form of *interface-type interface-number*
- As a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display gvrp statistics** to display the GVRP statistics of the specified trunk ports. If no ports are specified, this command displays the GVRP statistics for all trunk ports.

Examples

# Display GVRP statistics for trunk port GigabitEthernet 1/0/1.

```
<Sysname> display gvrp statistics interface gigabitethernet 1/0/1
```

```
GVRP statistics on port GigabitEthernet1/0/1

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

Table 46 Command output

Field	Description
GVRP Status	Indicates whether GVRP is enabled or disabled.
GVRP Running	Indicates whether GVRP is running.
GVRP Failed Registrations	Indicates the number of GVRP registration failures.
GVRP Last Pdu Origin	Indicates the source MAC address in the last GVRP PDU.
GVRP Registration Type	Indicates the GVRP registration mode (fixed, forbidden, or normal) on the port.

display gvrp status

Syntax

display gvrp status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display gvrp status** to display the global GVRP state.

Examples

# Display the global GVRP state.

```
<Sysname> display gvrp status

                GVRP is enabled
```

display gvrp vlan-operation

Syntax

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

View

Any view

Default level

0: Visit level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display gvrp vlan-operation** to display information about dynamic VLAN operations on a port.

Examples

# Display information about dynamic VLAN operations on GigabitEthernet 1/0/1.

```
<Sysname> display gvrp vlan-operation interface gigabitethernet 1/0/1
         Dynamic VLAN operations on port GigabitEthernet1/0/1

                 Operations of creating VLAN              :  2-100
                 Operations of deleting VLAN              :  none
                 Operations of adding VLAN to TRUNK       :  2-100
                 Operations of deleting VLAN from TRUNK   :  none
```

garp timer hold

Syntax

garp timer hold *timer-value*

undo garp timer hold

View

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

Default level

2: System level

Parameters

timer-value: Hold timer (in centiseconds), which must be a multiple of 5 and range from 10 (inclusive) to half the Join timer (inclusive).

Description

Use **garp timer hold** to set the GARP Hold timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use **undo garp timer hold** to restore the default of the GARP Hold timer. This may fail if the default is beyond the valid value range for the Hold timer.

By default, the Hold timer is 10 centiseconds.

Related commands: **display garp timer** and **garp timer join**.

Examples

# Set the GARP Hold timer to 15 centiseconds, assuming that the Join timer is 30 centiseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer hold 15
```

garp timer join

Syntax

garp timer join *timer-value*

undo garp timer join

View

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

Default level

2: System level

Parameters

timer-value: Join timer (in centiseconds), which must be a multiple of 5 and range from twice the Hold timer (inclusive) and half the Leave timer (inclusive).

Description

Use **garp timer join** to set the GARP Join timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use **undo garp timer join** to restore the default of the GARP Join timer. This may fail if the default is beyond the valid value range for the Join timer.

By default, the Join timer is set to 20 centiseconds.

Related commands: **display garp timer**, **garp timer hold**, and **garp timer leave**.

Examples

# Set the GARP Join timer to 25 centiseconds, assuming that both the Hold timer and the Leave timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer join 25
```

garp timer leave

Syntax

garp timer leave *timer-value*

undo garp timer leave

View

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

Default level

2: System level

Parameters

timer-value: Leave timer (in centiseconds), which must be a multiple of 5 and range from twice the Join timer (exclusive) to the LeaveAll timer (exclusive).

Description

Use **garp timer leave** to set the GARP Leave timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use **undo garp timer leave** to restore the default of the GARP Leave timer. This may fail if the default is beyond the valid value range for the Leave timer.

By default, the Leave timer is set to 60 centiseconds.

Related commands: **display garp timer**, **garp timer join**, and **garp timer leaveall**.

Examples

# Set the GARP Leave timer to 100 centiseconds, assuming that both the Join timer and the LeaveAll timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer leave 100
```

garp timer leaveall

Syntax

garp timer leaveall *timer-value*

undo garp timer leaveall

View

System view

Default level

2: System level

Parameters

timer-value: Leaveall timer (in centiseconds), which must be a multiple of 5 and range from the maximum Leave timer on the device (exclusive) to 32765 (inclusive).

Description

Use **garp timer leaveall** to set the GARP LeaveAll timer.

Use **undo garp timer leaveall** to restore the default. This may fail if the default is beyond the valid value range for the LeaveAll timer.

By default, the LeaveAll timer is 1000 centiseconds.

NOTE:

To keep the dynamic VLANs learned through GVRP stable, do not set the LeaveAll timer smaller than its default value.

Related commands: **display garp timer** and **garp timer leave**.

Examples

# Set the leaveall timer to 2000 centiseconds, assuming that the Leave timer on every port is set to 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 2000
```

gvrp

Syntax

gvrp

undo gvrp

View

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

Default level

2: System level

Parameters

None

Description

Use **gvrp** to enable GVRP.

Use **undo gvrp** to disable GVRP.

By default, GVRP is disabled.

Settings in system view take effect globally; settings in Ethernet view or Layer 2 aggregate interface take effect on the current interface; settings in port group view take effect on all ports in the port group.

To enable GVRP on a port, enable GVRP globally before you enable it on the port.

In interface view, you can use this command on trunk ports only.

You cannot change the link type of a GVRP-enabled trunk port.

Related commands: **display gvrp status**.

Examples

# Enable GVRP globally.

```
<Sysname> system-view
[Sysname] gvrp
GVRP is enabled globally.
```

gvrp registration

Syntax

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View

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

Default level

2: System level

Parameters

fixed: Sets the GVRP registration mode to fixed.

forbidden: Sets the GVRP registration mode to forbidden.

normal: Sets the GVRP registration mode to normal.

Description

Use **gvrp registration** to configure the GVRP registration mode.

Use **undo gvrp registration** to restore the default.

The default GVRP registration mode is normal.

Settings in system view take effect globally; settings in Ethernet view or Layer 2 aggregate interface take effect on the current interface; settings in port group view take effect on all ports in the port group.

This command is only available on trunk ports.

Related commands: **display garp statistics**.

Examples

# Set the GVRP registration mode to fixed on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] gvrp registration fixed
```

reset garp statistics

Syntax

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

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Clears the GARP statistics of one or multiple ports.

You can provide up to 10 port lists, specified in the following ways:

- As an individual port in the form of *interface-type interface-number*
- As a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start port number specified by *interface-number1*.

Description

Use **reset garp statistics** to clear the GARP statistics on the specified ports. If no ports are specified, this command clears the GARP statistics on all ports.

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

Related commands: **display garp statistics**.

Examples

# Clear the GARP statistics on all ports.

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

QinQ configuration commands

- Throughout this document, customer network VLANs (CVLANs), also called inner VLANs, refer to the VLANs that a customer uses on the private network; and service provider network VLANs (SVLANs), also called outer VLANs, refer to the VLANs that a service provider uses to carry VLAN tagged traffic for customers.
- Selective QinQ is achieved through QoS policies. For more information about QoS policy configuration commands, see *ACL and QoS Command Reference*.

qinq enable

Syntax

qinq enable

undo qinq enable

View

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

Default level

2: System level

Parameters

None

Description

Use **qinq enable** to enable basic QinQ on the Ethernet ports.

Use **undo qinq enable** to disable basic QinQ on the Ethernet ports.

By default, basic QinQ is disabled on Ethernet ports.

A basic QinQ-enabled port tags received frames with its PVID tag.

Configured in Layer 2 Ethernet interface view, the command takes effect on the port only. Configured in Layer 2 aggregate interface view, the command takes effect on the Layer 2 aggregate interface and all the member ports in the aggregation group. Configured in port group view, the command takes effect on all ports in the port group.

Examples

# Enable basic QinQ on GigabitEthernet 1/0/1.

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

# Enable basic QinQ on all ports in port group 1.

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

qinq ethernet-type

Syntax

qinq ethernet-type *hex-value*

undo qinq ethernet-type

View

System view

Default Level

2: System level

Parameters

hex-value: Hexadecimal TPID value, ranging from 0x0001 to 0xFFFF, excluding the common protocol type values listed in Table 47.

Table 47 Common protocol type values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E
Cluster	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Description

Use **qinq ethernet-type** to configure the TPID value in VLAN tags.

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

By default, the TPID value is 0x8100.

The TPID value configured on the 5120 EI switch applies to both the CVLAN tags and the SVLAN tags.

Examples

# Set the TPID value to 0x8200 globally.

```
<Sysname> system-view
[Sysname] qinq ethernet-type 8200
```

qinq transparent-vlan

Syntax

qinq transparent-vlan *vlan-list*

undo qinq transparent-vlan { **all** | *vlan-list* }

View

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

Default level

2: System level

Parameters

vlan-list: Specifies a list of existing VLANs in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where *vlan-id* represents the VLAN ID ranging from 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

all: Indicates all VLANs.

Description

Use **qinq transparent-vlan** to configure VLAN transparent transmission on one or multiple ports, so the port or ports can transparently transmit frames from the specified VLANs.

Use **undo qinq transparent-vlan** to remove the configuration.

By default, VLAN transparent transmission is not configured on ports.

Configured in Layer 2 Ethernet interface view, the command takes effect on the interface only. Configured in Layer 2 aggregate interface view, the command takes effect on the Layer 2 aggregate interface and all the member ports in the aggregation group. Configured in port group view, the command takes effect on all ports in the port group.

Examples

# Enable basic QinQ on GigabitEthernet 1/0/1, and configure GigabitEthernet 1/0/1 to transparently transmit frames from VLAN 2, VLAN 3, 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 3 50 to 100
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] qinq transparent-vlan 2 3 50 to 100
```

qinq vid

Syntax

qinq vid *vlan-id*

undo qinq vid *vlan-id*

View

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

Default level

2: System level

Parameters

vlan-id: Sets an outer VLAN ID, ranging from 1 to 4094.

Description

Use **qinq vid** to set the outer VLAN tag that the port adds to customer VLAN frames, and enter QinQ view.

Use **undo qinq vid** to remove all configurations corresponding to the outer VLAN ID performed in QinQ view.

By default, the outer VLAN tag is the port's PVID tag.

Configured in Layer 2 Ethernet interface view, the command takes effect on the interface only. Configured in Layer 2 aggregate interface view, the command takes effect on the Layer 2 aggregate interface and all the member ports in the aggregation group. Configured in port group view, the command takes effect on all ports in the port group.

An inner VLAN tag corresponds to only one outer VLAN tag. To change an outer VLAN tag, delete the old outer VLAN tagging policy and configure a new outer VLAN tag.

Related command: **raw-vlan-id inbound**.

Examples

# Enable basic QinQ on GigabitEthernet 1/0/1, configure GigabitEthernet 1/0/1 to tag frames with outer VLAN 10, and enter QinQ view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] qinq vid 10
[Sysname-GigabitEthernet1/0/1-vid-10]
```

# Enable basic QinQ on all ports in port group 1, configure them to tag frames with outer VLAN 10, and enter QinQ view.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet
1/0/6
[Sysname-port-group-manual-1] qinq enable
[Sysname-port-group-manual-1] qinq vid 10
[Sysname-port-group-manual-1-vid-10]
```

raw-vlan-id inbound

Syntax

raw-vlan-id inbound { **all** | *vlan-list* }

undo raw-vlan-id inbound { **all** | *vlan-list* }

View

QinQ view

Default level

2: System level

Parameters

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

all: Specifies all VLAN IDs.

Description

Use **raw-vlan-id inbound** to tag frames of the specified VLANs with the SVLAN.

Use **undo raw-vlan-id inbound** to remove the configuration.

By default, Ethernet ports do not tag VLAN frames with outer VLAN tags.

You can configure this command in the same view multiple times. A new configuration does not overwrite the previous ones and the configured values are automatically arranged in an ascending order.

Related commands: **qinq vid**.

Examples

# Enable basic QinQ on GigabitEthernet 1/0/1 and configure GigabitEthernet 1/0/1 to tag frames from VLAN 3, VLAN 5, and VLANs 20 through 100 with SVLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] qinq vid 100
[Sysname-GigabitEthernet1/0/1-vid-100] raw-vlan-id inbound 3 5 20 to 100
```

LLDP configuration commands

display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

global: Displays the global LLDP information to be sent.

interface *interface-type interface-number*: Displays the LLDP information to be sent out of the interface specified by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display lldp local-information** to display the LLDP information to be sent, which will be contained in the LLDP TLVs and sent to neighbor devices.

If no keyword or argument is specified, this command displays all LLDP information to be sent, including the global LLDP information and the LLDP information about the LLDP-enabled ports in the up state.

Examples

# Display all LLDP information to be sent.

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID         : 00e0-fc00-5600
  System name        : Sysname
  System description : HP Comware Platform Software
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  MED information
  Device class: Connectivity device
  (MED inventory information of master board)
  HardwareRev               : REV.A
  FirmwareRev               : 109
  SoftwareRev               : 5.20 Alpha 2101
  SerialNum                 : NONE
  Manufacturer name         : HP
  Model name                : HP Comware
  Asset tracking identifier : Unknown
LLDP local-information of port 1[GigabitEthernet1/0/1]:
  Port ID subtype  : Interface name
  Port ID          : GigabitEthernet1/0/1
  Port description : GigabitEthernet1/0/1 Interface

  Management address type           : ipv4
  Management address                : 192.168.1.11
  Management address interface type : IfIndex
  Management address interface ID   : 54
  Management address OID            : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001

  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : speed(1000)/duplex(Full)

  Power port class          : PSE
  PSE power supported       : Yes
  PSE power enabled         : Yes
  PSE pairs control ability : Yes
  Power pairs               : Signal
  Port power classification : Class 0
  Power type                : Type 2 PSE
  Power source              : Primary
  Power priority            : high
  PD requested power value  : 25.5(w)
  PSE allocated power value : 25.5(w)

  Link aggregation supported : Yes
  Link aggregation enabled   : No
  Aggregation port ID        : 0
```

```
Maximum frame Size: 1536

MED information
Media policy type        : Unknown
Unknown Policy           : Yes
VLAN tagged              : No
Media policy VlanID      : 0
Media policy L2 priority : 0
Media policy Dscp        : 0

PoE PSE power source      : Primary
Port PSE Priority         : high
Port available power value: 25.5(w)
```

Table 48 Command output

Field	Description
Global LLDP local-information	Global LLDP information to be sent.
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: • **Bridge**—Switching is supported. • **Router**—Routing is supported.
System capabilities enabled	Enabled capabilities: • **Bridge**—Switching is enabled. • **Router**—Routing is 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 function as a normal terminal device. • **Class III**—Communication terminal device. It supports the IP communication systems of end users, and can also function as a normal terminal device or media terminal device.
MED inventory information of master board	MED inventory information of the master of the IRF fabric.
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
LLDP local-information of port 1	LLDP information to be sent out of port 1.
Port ID subtype	Port ID type, which can be MAC address or interface name.
Port ID	Port ID, the value of which depends on the port ID subtype.

Field	Description
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 and protocol VLAN ID(PPVID)	Port protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether or not protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether or not protocol VLAN is enabled on the port.
VLAN name of VLAN 1	Name of VLAN 1.
Auto-negotiation supported	Indicates whether or not auto-negotiation is supported on the port.
Auto-negotiation enabled	Indicates whether or not auto-negotiation is enabled on the port.
OperMau	Speed and duplex state of the port.
PoE supported	Indicates whether or not PoE is supported on the port.
Power port class	PoE device type: • **PSE**—Power sourcing equipment • **PD**—Powered device
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode: • **Signal**—PoE via signal lines • **Spare**—PoE via spare lines
Port power classification	Port power classification of the PD: • Class 0 • Class 1 • Class 2 • Class 3 • Class 4
Power type	This field appears only on the devices that support PoE+. PoE device type • Type 1 PSE—Provides a power of 0 W to 15.4 W, a voltage of 44 V to 57 V, and a current of up to 350 mA. • Type 2 PSE, Provides a power of 0 W to 30 W, a voltage of 50 V to 57 V, and a current of up to 600 mA.
Power source	This field appears only on the devices that support PoE+. PSE power type: • **Unknown**—Unknown power supply • **Primary**—Primary power supply • **Backup**—Backup power supply

Field	Description
Power priority	This field appears only on the devices that support PoE+. PoE power supply priority of PSE ports: - Unknown - Critical - High - Low
PD requested power value	This field appears only on the devices that support PoE+. Power (in W) that the PD requests.
PSE allocated power value	This field appears only on the devices that support PoE+. Power (in W) that the PSE provides to the PD.
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 when link aggregation is disabled.
MED information	MED LLDP information.
Media policy type	Media policy type: - unknown - voice - voiceSignaling - guestVoice - guestVoiceSignaling - softPhoneVoice - videoconferencing - streamingVideo - videoSignaling
Unknown Policy	Indicates whether or not the media policy is unknown.
VLAN tagged	Indicates whether or not packets of the media VLAN are tagged.
Media Policy VlanID	ID of the media VLAN.
Media Policy L2 priority	Layer 2 priority.
Media Policy Dscp	DSCP precedence.
Location format	Location information format: - **Invalid**—The format of the location information is invalid. - **Coordinate-based LCI**—The location information is coordinate-based. - **Civic Address LCI**—Typical address information. - **ECS ELIN**—Telephone number for urgencies.
PoE PSE power source	PSE power type: - **Unknown**—Unknown power supply - **Primary**—Primary power supply - **Backup**—Backup power supply

Field	Description
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.

display lldp neighbor-information

Syntax

display lldp neighbor-information [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays the summary of LLDP information sent from the neighboring devices. If this keyword is not specified, this command displays detailed LLDP information sent from the neighboring devices.

interface *interface-type interface-number*: Displays the LLDP information sent from the neighboring devices received through a port specified by its type and number. If this option is not specified, this command displays the LLDP information sent from the neighboring devices received through all ports.

list: Displays the LLDP information sent from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information sent from a neighboring device specified by its system name. The *system-name* argument is a character string of 1 to 255 characters. If this option is not specified, this command displays the LLDP information sent from all neighboring devices in a list.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display lldp neighbor-information** to display the LLDP information carried in LLDP TLVs sent from the neighboring devices.

Examples

# Display the LLDP information sent from the neighboring devices received through all ports.

```
<Sysname> display lldp neighbor-information

LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor index   : 1
  Update time      : 0 days,0 hours,1 minutes,1 seconds
  Chassis type     : MAC address
  Chassis ID       : 000f-0055-0002
  Port ID type     : Interface name
  Port ID          : GigabitEthernet1/0/1
  Port description : GigabitEthernet1/0/1 Interface
  System name        : HP
  System description : HP Comware Platform Software
  System capabilities supported : Repeater,Bridge,Router
  System capabilities enabled   : Repeater,Bridge,Router

  Management address type           : ipv4
  Management address                : 192.168.1.55
  Management address interface type : IfIndex
  Management address interface ID   : Unknown
  Management address OID            : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001

  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : speed(1000)/duplex(Full)

  Power port class          : PD
  PSE power supported       : No
  PSE power enabled         : No
  PSE pairs control ability : No
  Power pairs               : Signal
  Port power classification : Class 0
  Power type                : Type 2 PD
  Power source              : PSE and local
  Power priority            : high
  PD requested power value  : 25.5(w)
  PSE allocated power value : 25.5(w)

  Link aggregation supported : Yes
  Link aggregation enabled   : No
  Aggregation port ID        : 0

  Maximum frame Size: 1536
```

# Display the LLDP information sent from all neighboring devices in a list.

```
<Sysname> display lldp neighbor-information list

System Name          Local Interface Chassis ID     Port ID
System1              GE1/0/1         000f-e25d-ee91 GigabitEthernet1/0/5
System2              GE1/0/2         000f-e25d-ee92 GigabitEthernet1/0/6
System3              GE1/0/3         000f-e25d-ee93 GigabitEthernet1/0/7
```

Table 49 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.
Chassis type	Chassis information: • Chassis component • Interface alias • Port component • MAC address • Network address (the IP address type, such as **ipv4**) • Interface name • **Locally assigned**—Local configuration
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface or some other value depending on the chassis type.
Port ID type	Port information: • Interface alias • Port component • MAC address • Network address (the IP address type, such as **ipv4**) • Interface name • Agent circuit ID • **Locally assigned**—Local configuration
Port ID	Value of the port ID type.
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. • **Router**—Routing is supported.
System capabilities enabled	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **Router**—Routing is enabled.
Management address OID	Management address object ID.
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID.

Field	Description
Port and protocol VLAN supported	Indicates whether or not protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether or not protocol VLAN is enabled on the port.
VLAN name of VLAN 1	Name of VLAN 1.
Auto-negotiation supported	Indicates whether or not auto-negotiation is supported on the port.
Auto-negotiation enabled	Indicates whether or not auto-negotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Power port class	PoE device type: • **PSE**—Power sourcing equipment • **PD**—Powered device
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode: • **Signal**—PoE via signal lines • **Spare**—PoE via spare lines
Port power classification	Port power classification of the PD: • Class 0 • Class 1 • Class 2 • Class 3 • Class 4
Power type	This field appears only on the devices that support PoE+. PoE device type: • **Type 1 PD**—Receives a power of 0 W to 15.4 W, a voltage of 44 V to 57 V, and a current of up to 350 mA. • **Type 2 PD**—Receives a power of 0 W to 30 W, a voltage of 50 V to 57 V, and a current of up to 600 mA.
Power source	This field appears only on the devices that support PoE+. PD power type: • **Unknown**—Unknown power supply • **PSE**—PSE power supply • **Local**—Local power supply • **PSE and local**—PSE and local power supplies
Power priority	This field appears only on the devices that support PoE+. PoE power receiving priority of PD ports: • Unknown • Critical • High • Low
PD requested power value	This field appears only on the devices that support PoE+. Power (in W) that the PD requests.

Field	Description
PSE allocated power value	This field appears only on the devices that support PoE+. Power (in W) that the PSE provides to the PD.
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 when link aggregation is disabled.
Location format	Location information format: • **Invalid**—The format of the location information is invalid. • **Coordinate-based LCI**—The location information is coordinate-based. • **Civic Address LCI**—Typical address information. • **ECS ELIN**—Telephone for urgencies.
PoE PSE power source	PSE power type: • **Unknown**—Unknown power supply • **Primary**—Primary power supply • **Backup**—Backup power supply
PoE PD power source	PD power type: • **Unknown**—Unknown power supply • **PSE**—PSE power supply • **Local**—Local power supply • **PSE and local**—PSE and local power supplies
Port PSE Priority	PoE power supply priority of PSE ports: • Unknown • Critical • High • Low
Port PD Priority	PoE power receiving priority of PD ports: • Unknown • Critical • High • Low
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, 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.
TLV information	Information contained in unknown organizationally specific TLV.
Local Interface	Local port that receives the LLDP information.

display lldp statistics

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

global: Displays the global LLDP statistics.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display lldp statistics** to display the global LLDP statistics or the LLDP statistics of a port.

If no keyword or argument is specified, this command displays the global LLDP statistics as well as the LLDP statistics of all ports.

Examples

# Display the global LLDP statistics as well as 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]:
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 50 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time the neighbor information was last updated.
The number of LLDP neighbor information inserted	Number of times of adding neighbor information.
The number of LLDP neighbor information deleted	Number of times of removing neighbor information.
The number of LLDP neighbor information dropped	Number of times of dropping neighbor information due to lack of available memory space.

display lldp status

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display lldp status** to display LLDP status information.

If no port is specified, this command displays the global LLDP status and the LLDP status information for all ports.

Examples

# Display the global LLDP status as well as the LLDP status information of all ports.

```
<Sysname> display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 0
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days,0 hours,4 minutes,40 seconds
Transmit interval              : 30s
Hold multiplier                : 4
```

```
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3
Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP            : Enable
Admin status                   : Tx_Rx
Trap flag                      : No
Polling interval               : 0s

Number of neighbors            : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 23
Number of received unknown TLV : 0
```

Table 51 Command output

Field	Description
Global status of LLDP	Indicates whether or not LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDPDU transmit interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP re-initialization delay.
Transmit delay	LLDPDU transmit delay.
Trap interval	Trap transmit interval.
Fast start times	Number of the LLDPDUs sent each time fast LLDPDU transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether or not LLDP is enabled on the port.
Admin status	LLDP mode of the port: • **TxRx**—The port sends and receives LLDPDUs. • **Rx_Only**—The port only receives LLDPDUs. • **Tx_Only**—The port only sends LLDPDUs. • **Disable**—The port does not send or receive LLDPDUs.
Trap Flag	Indicates whether or not 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 LLDPDU sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in all received LLDPDUs.

display lldp tlv-config

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

If no port is specified, this command displays the types of advertisable optional TLVs of each port.

Examples

# Display the types of advertisable optional LLDP TLVs of interface GigabitEthernet 1/0/1.

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
NAME                              STATUS    DEFAULT
Basic optional TLV:
Port Description TLV              YES       YES
System Name TLV                   YES       YES
System Description TLV            YES       YES
System Capabilities TLV           YES       YES
Management Address TLV            YES       YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV                  YES       YES
Port And Protocol VLAN ID TLV     YES       YES
VLAN Name TLV                     YES       YES

IEEE 802.3 extend TLV:
MAC-Physic TLV                    YES       YES
Power via MDI TLV                 YES       YES
Link Aggregation TLV              YES       YES
Maximum Frame Size TLV            YES       YES
```

```
LLDP-MED extend TLV:
Capabilities TLV                  YES        YES
Network Policy TLV                YES        YES
Location Identification TLV       NO         NO
Extended Power via MDI TLV        YES        YES
Inventory TLV                     YES        YES
```

Table 52 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether or not a specific type of TLV is sent through a port.
DEFAULT	Indicates whether or not a specific type of TLV is sent through a port by default.
Basic optional TLV	Basic TLVs: • Port description TLV • System name TLV • System description TLV • System capabilities TLV • Management address TLV
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: • Port VLAN ID TLV • Port and protocol VLAN ID TLV • VLAN name 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, including hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV, and asset id TLV

lldp admin-status

Syntax

lldp admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp admin-status

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

disable: Specifies the **Disable** mode. A port in this mode does not send or receive LLDPDUs.

rx: Specifies the **Rx** mode. A port in this mode only receives LLDPDUs.

tx: Specifies the **Tx** mode. A port in this mode only sends LLDPDUs.

txrx: Specifies the **TxRx** mode. A port in this mode sends and receives LLDPDUs.

Description

Use **lldp admin-status** to specify the LLDP operating mode for a port or all ports in a port group.

Use **undo lldp admin-status** to restore the default LLDP operating mode.

By default, the LLDP operating mode is **TxRx**.

Examples

# Configure the LLDP operating mode as **Rx** for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp admin-status rx
```

lldp check-change-interval

Syntax

lldp check-change-interval *interval*

undo lldp check-change-interval

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

interval: Sets the LLDP polling interval, ranging from 1 to 30 seconds.

Description

Use **lldp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo lldp check-change-interval** to restore the default.

By default, LLDP polling is disabled.

Examples

# Enable LLDP polling on GigabitEthernet 1/0/1, setting the polling interval to 30 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp check-change-interval 30
```

lldp compliance admin-status cdp

Syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

undo lldp compliance admin-status cdp

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

disable: Specifies the disable mode, where CDP-compatible LLDP cannot receive or transmit CDP packets.

txrx: Specifies the TxRx mode, where CDP-compatible LLDP can send and receive CDP packets.

Description

Use **lldp compliance admin-status cdp** to configure the operating mode of CDP-compatible LLDP on a port or port group.

Use **undo lldp compliance admin-status cdp** to restore the default.

By default, CDP-compatible LLDP operates in disable mode.

For your device to work with Cisco IP phones, you must enable CDP-compatible LLDP globally and then configure CDP-compatible LLDP to operate in TxRx mode on the specified ports.

Related commands: **lldp compliance cdp**.

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

lldp compliance cdp

Syntax

lldp compliance cdp

undo lldp compliance cdp

View

System view

Default level

2: System level

Parameters

None

Description

Use **lldp compliance cdp** to enable global CDP compatibility.

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

By default, CDP compatibility is globally disabled.

Because the maximum TTL allowed by CDP is 255 seconds, the TTL configuration must be no more than 255 seconds for CDP-compatible LLDP to operate with Cisco IP phones. The TTL configuration is the product of the TTL multiplier and the LLDPDU transmit interval.

Related commands: **lldp hold-multiplier** and **lldp timer tx-interval**.

Examples

# Enable LLDP to be compatible with CDP globally.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
```

lldp enable

Syntax

lldp enable

undo lldp enable

View

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

Default level

2: System level

Parameters

None

Description

Use **lldp enable** to enable LLDP.

Use **undo lldp enable** to disable LLDP.

By default, LLDP is enabled on a port, and enabled globally.

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
```

lldp encapsulation snap

Syntax

lldp encapsulation snap

undo lldp encapsulation

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **lldp encapsulation snap** to configure the encapsulation format for LLDPDUs as SNAP on a port or a group of ports.

Use **undo lldp encapsulation** to restore the default encapsulation format for LLDPDUs.

By default, the encapsulation format for LLDPDUs is Ethernet II.

NOTE:

The command does not apply to LLDP-CDP packets, which use only SNAP encapsulation.

Examples

# Configure the encapsulation format for LLDPDUs as SNAP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

View

System view

Default level

2: System level

Parameters

count: Sets the number of the LLDPDUs sent each time fast LLDPDU transmission is triggered. The argument ranges from 1 to 10.

Description

Use **lldp fast-count** to set the number of the LLDPDUs sent each time fast LLDPDU transmission is triggered.

Use **undo lldp fast-count** to restore the default.

By default, the number is 3.

Examples

# Configure the device to send four LLDPDUs each time fast LLDPDU transmission is triggered.

```
<Sysname> system-view
[Sysname] lldp fast-count 4
```

lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

View

System view

Default level

2: System level

Parameters

value: Sets the TTL multiplier, ranging from 2 to 10.

Description

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier to** restore the default.

By default, the TTL multiplier is 4.

You can set the TTL of the local device information by configuring the TTL multiplier.

The TTL configuration of a device is determined by the following expression:

TTL multiplier × LLDPDU transmit interval

The TTL can be up to 65535 seconds. Longer TTLs will be rounded off to 65535 seconds.

Related commands: **lldp timer tx-interval**.

Examples

# Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

lldp management-address-format string

Syntax

lldp management-address-format string

undo lldp management-address-format

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **lldp management-address-format string** to encapsulate the management address in the form of strings in TLVs.

Use **undo lldp management-address-format** to restore the default.

By default, the management address is encapsulated in the form of numbers in TLVs.

Examples

# Configure GigabitEthernet 1/0/1 to encapsulate the management address in the form of strings in management address TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address-format string
```

lldp management-address-tlv

Syntax

lldp management-address-tlv [*ip-address*]

undo lldp management-address-tlv

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

ip-address: Specifies a management address to be advertised in LLDPDUs.

Description

Use **lldp management-address-tlv** to enable management address advertising and set the management address.

Use **undo lldp management-address-tlv** to disable management address advertising in LLDPDUs.

By default, the management address is advertised through LLDPDUs. The management address is the main IP address of the lowest-ID VLAN carried on the port. If none of the carried VLANs is assigned an IP address, no management address will be advertised.

An LLDPDU carries only one management address TLV. If you set the management address repeatedly, the latest one takes effect.

If you run the **lldp management-address-tlv** command without specifying the *ip-address* argument, the advertised management address is the main IP address of the lowest-ID VLAN carried on the interface. If none of the carried VLANs is assigned an IP address, no management address will be advertised.

Examples

# Set the management address to 192.6.0.1 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address-tlv 192.6.0.1
```

lldp notification remote-change enable

Syntax

lldp notification remote-change enable

undo lldp notification remote-change enable

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **lldp notification remote-change enable** to enable LLDP trapping for a port or all ports in a port group.

Use **undo lldp notification remote-change enable** to restore the default.

By default, LLDP trapping is disabled on ports.

Examples

# Enable LLDP trapping for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification remote-change enable
```

lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

View

System view

Default level

2: System level

Parameters

interval: Sets the LLDP trap transmit interval, ranging from 5 to 3600 seconds.

Description

Use **lldp timer notification-interval** to set the LLDP trap transmit interval.

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

By default, the LLDP trap transmit interval is 5 seconds.

Examples

# Set the LLDP trap transmit interval to 8 seconds.

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

lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

View

System view

Default level

2: System level

Parameters

delay: Sets the LLDP re-initialization delay, ranging from 1 to 10 seconds.

Description

Use **lldp timer reinit-delay** to set the LLDP re-initialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

By default, the LLDP re-initialization delay is 2 seconds.

Examples

# Set the LLDP re-initialization delay to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer tx-delay

Syntax

lldp timer tx-delay *delay*

undo lldp timer tx-delay

View

System view

Default level

2: System level

Parameters

delay: Sets the LLDPDU transmit delay, ranging from 1 to 8192 seconds.

Description

Use **lldp timer tx-delay** to set the LLDPDU transmit delay.

Use **undo lldp timer tx-delay** to restore the default.

By default, the LLDPDU transmit delay is 2 seconds.

It is a good practice to set the LLDPDU transmit delay to be no greater than a quarter of the LLDPDU transmit interval.

If the LLDPDU transmit delay is greater than the LLDPDU transmit interval, the device uses the LLDPDUs transmit delay as the transmit interval.

Related commands: **lldp timer tx-interval**.

Examples

# Set the LLDPDU transmit delay to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-delay 4
```

lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

View

System view

Default level

2: System level

Parameters

interval: Sets the LLDPDU transmit interval, ranging from 5 to 32768 seconds.

Description

Use **lldp timer tx-interval** to set the LLDPDU transmit interval.

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

By default, the LLDPDU transmit interval is 30 seconds.

It is a good practice to set the LLDPDU transmit interval to be no less than four times the LLDPDU transmit delay.

If the LLDPDU transmit interval is less than the LLDPDU transmit delay, the device uses the LLDPDUs transmit delay as the transmit interval.

Related commands: **lldp timer tx-delay**.

Examples

# Set the LLDPDU transmit interval to 20 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

lldp tlv-enable

Syntax

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } | **network-policy** | **power-over-ethernet** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** } | **dot3-tlv** { **all** |

link-aggregation | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** | **network-policy** | **power-over-ethernet** } }

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

all: Advertises all basic LLDP TLVs, IEEE 802.1 organizationally specific LLDP TLVs, or IEEE 802.3 organizationally specific LLDP TLVs when the **all** keyword is specified for **basic-tlv**, **dot1-tlv**, or **dot3-tlv**; or advertises all LLDP-MED TLVs except location identification TLVs when the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP 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: Advertises port and protocol VLAN ID TLVs.

vlan-name: Advertises VLAN name TLVs.

vlan-id: Specifies a VLAN ID in the TLVs to be advertised. The argument ranges from 1 to 4094 and defaults to the least VLAN ID on the port.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

link-aggregation: Advertises link aggregation TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power via 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 normal address information about the network device in location identification TLVs .

device-type: Sets a device type value, ranging from 0 to 2. Value 0 specifies a DHCP server. Value 1 specifies a switch. Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code, corresponding to ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information, where *ca-type* represents the address information type, ranging from 0 to 255, *ca-value* represents address information, a string of 1 to 250 characters, and &<1-10> indicates that you can enter up to 10 parameters.

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: Advertises network policy TLVs.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Description

Use **lldp tlv-enable** to configure the types of advertisable TLVs for a port or all ports in a port group.

Use **undo lldp tlv-enable** to disable the advertising of specific types of TLVs.

By default, the device can advertise on a Layer 2 Ethernet port all types of LLDP TLVs, except location identification TLVs.

To enable the device to advertise LLDP-MED TLVs, you must first enable it to advertise LLDP-MED capabilities TLVs.

To disable the device from advertising LLDP-MED capabilities TLVs, you must first disable it from advertising other LLDP-MED TLVs.

To disable the device from advertising MAC/PHY configuration/status TLVs, you must first disable it from advertising LLDP-MED capabilities TLVs.

If you enable the device to advertise LLDP-MED capabilities TLVs, you also enable it to advertise MAC/PHY configuration/status TLVs.

To enable the device to advertise multiple types of TLVs, you can execute the **lldp tlv-enable** command repeatedly without the **all** keyword specified.

Examples

# Enable the device to advertise link aggregation TLVs of the IEEE 802.3 organizationally specific TLVs on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

lldp voice-vlan

Syntax

lldp voice-vlan *vlan-id*

undo lldp voice-vlan

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

vlan-id: Specifies a voice VLAN by its ID, which ranges from 1 to 4094.

Description

Use **lldp voice-vlan** *vlan-id* to configure a port to advertise a specific voice VLAN ID to the connected IP phone through LLDP. If CDP compatibility is enabled, LLDP also includes the specified voice VLAN ID in the CDP packets sent to the IP phone.

Use **undo lldp voice-vlan** to restore the default.

By default, if a voice VLAN is configured on an LLDP-enabled port, LLDP advertises this voice VLAN to the IP phone connected to the port.

Examples

# Configure port GigabitEthernet 1/0/1 to advertise voice VLAN 4094.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp voice-vlan 4094
```

voice vlan track lldp

Syntax

voice vlan track lldp

undo voice vlan track lldp

View

System view

Default level

2: System level

Parameters

None

Description

Use **voice vlan track lldp** to enable LLDP to automatically discover IP phones.

Use **undo voice vlan track lldp** to disable LLDP from automatically discovering IP phones.

By default, LLDP is disabled from automatically discovering IP phones.

Examples

# Enable the switch to automatically discover IP phones through LLDP.

```
<Sysname> system-view
[Sysname] voice vlan track lldp
```

MVRP commands

display mvrp running-status

Syntax

display mvrp running-status [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 *interface-type interface-number1* [**to** *interface-type interface-number2*] parameters. If this option is not specified, this command displays MVRP running status of all MVRP-enabled trunk ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mvrp running-status** to display the MVRP running status.

Examples

# Display the MVRP running status of all ports.

```
<Sysname> display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                       : Enabled
 Running Status                       : Enabled
 Join Timer                           : 20 (centiseconds)
 Leave Timer                          : 60 (centiseconds)
 Periodic Timer                       : 100 (centiseconds)
 LeaveAll Timer                       : 1000 (centiseconds)
 Registration Type                    : Normal
```

```
Local VLANs :
 1(default), 2-10,
```

Table 53 Command output

Field	Description
MVRP Global Info	Global MVRP information.
Global Status	Global MVRP status: - Enabled - Disabled
Compliance-GVRP	GVRP compatibility status: - **True**—Compatible - **False**—Incompatible
----[GigabitEthernet1/0/1] ----	Interface prompt. The information between the current interface prompt and the next interface prompt is information about the current interface.
Config Status	Whether MVRP is enabled on the port: - Enabled - Disabled
Running Status	Whether MVRP takes effect on the port (determined by the link state and MVRP enabling status of the port): - Enabled - Disabled
Join Timer	Join timer, in centiseconds.
Leave Timer	Leave timer, in centiseconds.
Periodic Timer	Periodic timer, in centiseconds.
LeaveAll Timer	LeaveAll timer, in centiseconds.
Registration Type	MVRP registration mode: - Fixed - Forbidden - Normal
Local VLANs	VLAN information in the local database, which displays the VLANs learned through MVRP.

display mvrp state

Use **display mvrp state** to display the MVRP state of an interface in a VLAN.

Syntax

display mvrp state interface *interface-type interface-number* **vlan** *vlan-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the MVRP state of an interface specified by its type and number.

vlan *vlan-id*: Displays the MVRP state of an interface in an VLAN specified by its VLAN ID, which ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mvrp state** to display the MVRP state of an interface in a VLAN.

Examples

# Display the MVRP state of port GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> display mvrp state interface gigabitethernet 1/0/1 vlan 2
MVRP state of VLAN 2 on port GE1/0/1
    Port      VLAN   App-state   Reg-state
 ----------- ------ ----------- -----------
 GE1/0/1          2       VP          IN
```

Table 54 Command output

Field	Description
MVRP state of VLAN 2 on port GE1/0/1	MVRP state of GigabitEthernet 1/0/1 in VLAN 2.

Field	Description
App-state	Declaration state, which indicates the state of the attribute that the local participant declares to the remote participant. The state can be VO, VP, VN, AN, AA, QA, LA, AO, QO, AP, QP, or LO. Each state consists of two letters. The first letter indicates the state: • **V**—Very anxious, which means that the local participant has not declared the attribute or has not received any Join message containing the attribute. • **A**—Anxious, which means that the local participant has declared the attribute once or has received one Join message containing the attribute. • **Q**—Quiet, which means that the local participant has declared the attribute two times, the local participant has declared the attribute once and has received one Join message containing the attribute, or the local participant has received two Join messages containing the attribute. • **L**—Leaving, which means that the local participant is deregistering the attribute. The second letter indicates the membership state: • **A**—Active member, which means that the local participant is declaring the attribute, has sent at least one Join message containing the attribute, and may receive Join messages. • **P**—Passive member, which means that the local participant is declaring the attribute, has received Join messages containing the attribute, but has not sent Join messages containing the attribute. • **O**—Observer, which means that the local participant is not declaring the attribute but is monitoring the attribute. • **N**—New, which means that the local participant is declaring the attribute, is receiving the Join message containing the attribute, but is not sending Join messages for the attribute. For example, VP indicates "Very anxious, Passive member".
Reg-state	Registration state of the attribute declared by remote participants on the local participant. The state can be IN, LV, or MT: • **IN**—Registered. • **LV**—Previously registered, but now being timed out. • **MT**—Not registered.

display mvrp statistics

Syntax

display mvrp statistics [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, this command displays MVRP statistics of all MVRP-enabled trunk ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mvrp statistics** to display MVRP statistics.

Examples

# Display MVRP statistics of all ports.

```
<Sysname> display mvrp statistics

 ----[GigabitEthernet1/0/1]----
 Failed Registrations           : 1
 Last PDU Origin                : 000f-e200-0010
 Frames Received                : 201
  New Event Received                 : 0
  JoinIn Event Received              : 1167
  In Event Received                  : 0
  JoinMt Event Received              : 22387
  Mt Event Received                  : 31
  Leave Event Received               : 210
  LeaveAll Event Received            : 63
 Frames Transmitted             : 47
  New Event Transmitted              : 0
  JoinIn Event Transmitted           : 311
  In Event Transmitted               : 0
  JoinMt Event Transmitted           : 873
  Mt Event Transmitted               : 11065
  Leave Event Transmitted            : 167
  LeaveAll Event Transmitted         : 4
 Frames Discarded               : 0

 ----[GigabitEthernet1/0/2]----
 Failed Registrations           : 0
 Last PDU Origin                : 0000-0000-0000
 Frames Received                : 0
  New Event Received                 : 0
  JoinIn Event Received              : 0
  In Event Received                  : 0
  JoinMt Event Received              : 0
  Mt Event Received                  : 0
  Leave Event Received               : 0
  LeaveAll Event Received           : 0
 Frames Transmitted             : 0
  New Event Transmitted             : 0
  JoinIn Event Transmitted          : 0
  In Event Transmitted              : 0
  JoinMt Event Transmitted          : 0
  Mt Event Transmitted              : 0
  Leave Event Transmitted           : 0
  LeaveAll Event Transmitted        : 0
 Frames Discarded               : 0
```

Table 55 Command output

Field	Description
---[GigabitEthernet1/0/1]---	Interface prompt. The statistics between the current interface prompt and the next interface prompt are statistics of the current interface.
Failed Registrations	Number of VLAN registration failures through MVRP on the local participant.
Last PDU Origin	Source MAC address of the last MVRP PDU.
Frames Received	Number of MVRP protocol packets received
New Event Received	Number of New attribute events received.
JoinIn Event Received	Number of JoinIn attribute events received.
In Event Received	Number of In attribute events received.
JoinMt Event Received	Number of JoinMt attribute events received.
Mt Event Received	Number of Mt attribute events received.
Leave Event Received	Number of Leave attribute events received.
LeaveAll Event Received	Number of LeaveAll attribute events received.
Frames Transmitted	Number of MVRP protocol packets sent.
New Event Transmitted	Number of New attribute events sent.
JoinIn Event Transmitted	Number of JoinIn attribute events sent.
In Event Transmitted	Number of In attribute events sent.
JoinMt Event Transmitted	Number of JoinMt attribute events sent.
Mt Event Transmitted	Number of Mt attribute events sent.
Leave Event Transmitted	Number of Leave attribute events sent.
LeaveAll Event Transmitted	Number of LeaveAll attribute events sent.
Frames Discarded	Number of MVRP protocol packets dropped.

display mvrp vlan-operation

Syntax

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

View

Any view

Default level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the dynamic VLAN operations of an interface specified its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mvrp vlan-operation** to display the dynamic VLAN operations of an interface.

These dynamic VLANs refer to the VLANs that are dynamically learned through MVRP and have not taken effect on the local device.

If a dynamic VLAN learned through MVRP is an existing static VLAN on the device or a VLAN reserved for a protocol, the dynamic VLAN does not take effect on the local device.

Examples

# Display the dynamic VLAN operations of GigabitEthernet 1/0/1.

```
<Sysname> display mvrp vlan-operation interface gigabitethernet 1/0/1
 Dynamic VLAN operations on port GigabitEthernet1/0/1
  Operations of creating VLAN:  2-100
  Operations of deleting VLAN:  none
  Operations of adding VLAN to Trunk:  2-100
  Operations of deleting VLAN from Trunk:  none
```

Table 56 Command output

Field	Description
Operations of adding VLAN to Trunk	Operations of adding VLANs to trunk ports
Operations of deleting VLAN from Trunk	Operations of removing VLAN from trunk ports

mrp timer join

Syntax

mrp timer join *timer-value*

undo mrp timer join

View

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

Default level

2: System level

Parameters

timer-value: Join timer value (in centiseconds). The Join timer must be less than half the Leave timer, and must be a multiple of 20.

Description

Use **mrp timer join** to set the Join timer.

Use **undo mrp timer join** to restore the default.

By default, the Join timer is 20 centiseconds.

You will fail to restore the default Join timer if the default Join timer is not less than half the Leave timer.

Related commands: **display mvrp running-status** and **mrp timer leave**.

Examples

# Set the Join timer to 40 centiseconds. (Suppose the Leave timer is 100 centiseconds)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer join 40
```

mrp timer leave

Syntax

mrp timer leave *timer-value*

undo mrp timer leave

View

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

Default level

2: System level

Parameters

timer-value: Leave timer value (in centiseconds). The Leave timer must be greater than two times the Join timer, less than the LeaveAll timer, and a multiple of 20.

Description

Use **mrp timer leave** to set the Leave timer.

Use **undo mrp timer leave** to restore the default.

By default, the Leave timer is 60 centiseconds.

You will fail to restore the default Leave timer if the default Leave timer is not greater than two times the Join timer or not less than the LeaveAll timer.

Related commands: **display mvrp running-status**, **mrp timer join**, and **mrp timer leaveall**.

Examples

# Set the Leave timer to 100 centiseconds. (Suppose the Join and LeaveAll timer use their default settings)

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

```
[Sysname-GigabitEthernet1/0/1] mrp timer leave 100
```

mrp timer leaveall

Syntax

mrp timer leaveall *timer-value*

undo mrp timer leaveall

View

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

Default level

2: System level

Parameter

timer-value: LeaveAll timer value (in centiseconds). The LeaveAll timer must be greater than any Leave timer on each port, no greater than 32760, and a multiple of 20.

Description

Use **mrp timer leaveall** to set the LeaveAll timer.

Use **undo mrp timer leaveall** to restore the default.

By default, the LeaveAll timer is 1000 centiseconds.

You will fail to restore the default LeaveAll timer if the default LeaveAll timer is not greater than any Leave timer on each port.

Each time when the LeaveAll timer of a port expires, all attributes of the MSTIs on the port are deregistered throughout the network, and such a deregistration affects a large portion of the network. Do not set too small a value for the LeaveAll timer, and make sure that the LeaveAll timer is greater than any Leave timer on each port.

To keep the dynamic VLANs learned through MVRP stable, do not set the LeaveAll timer smaller than its default value (1000 centiseconds).

To avoid the case that the LeaveAll timer of a fixed participant always first expires, the switch randomly changes the LeaveAll timer within a certain range when the MRP participant restarts its LeaveAll timer.

Related commands: **display mvrp running-status** and **mrp timer leave**.

Examples

# Set the LeaveAll timer to 1500 centiseconds. (Suppose the Leave timer is restored to the default)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leaveall 1500
```

mrp timer periodic

Syntax

mrp timer periodic *timer-value*

undo mrp timer periodic

Default

The Periodic timer is 100 centiseconds.

View

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

Default level

2: System level

Parameters

timer-value: Periodic timer (in centiseconds), which can be 0 or 100. Setting the Periodic timer to 0 disables periodic transmission of MRP messages.

Description

Use **mrp timer periodic** to set the Periodic timer.

Use **undo mrp timer periodic** to restore the default.

By default, the Periodic timer is 100 centiseconds.

Related commands: **display mvrp running-status**.

Examples

# Set the Periodic timer to 0 centiseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer periodic 0
```

mvrp global enable

Syntax

mvrp global enable

undo mvrp global enable

View

System view

Default level

2: System level

Description

Use **mvrp global enable** to enable MVRP globally.

Use **undo mvrp global enable** to restore the default.

By default, MVRP is disabled globally.

Disabling MVRP globally also disables MVRP on all ports.

Related commands: **display mvrp running-status** and **mvrp enable**.

Examples

# Enable MVRP globally.

```
<Sysname> system-view
[Sysname] mvrp global enable
```

mvrp enable

Syntax

mvrp enable

undo mvrp enable

View

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

Default level

2: System level

Description

Use **mvrp enable** to enable MVRP on a port.

Use **undo mvrp enable** to disable MVRP on a port.

By default, MVRP is disabled on a port.

To enable MVRP on a port, first enable MVRP globally.

Disabling MVRP globally also disables MVRP on each port.

This command is available only on trunk ports.

You cannot change the link type of MVRP-enabled trunk port.

Related commands: **display mvrp running-status** and **mvrp global enable**.

Examples

# Configure GigabitEthernet 1/0/1 as a trunk port, and enable MVRP on it.

```
<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 all
[Sysname-GigabitEthernet1/0/1] mvrp enable
```

mvrp gvrp-compliance

Syntax

mvrp gvrp-compliance enable

undo mvrp gvrp-compliance enable

View

System view

Default level

2: System level

Description

Use **mvrp gvrp-compliance enable** to enable GVRP compatibility, so that the device can process both MVRP protocol packets and GVRP protocol packets.

Use **undo mvrp gvrp-compliance enable** to restore the default.

By default, GVRP compatibility is disabled.

Examples

# Enable GVRP compatibility.

```
<Sysname> system-view
[Sysname] mvrp gvrp-compliance enable
```

mvrp registration

Syntax

mvrp registration { **fixed** | **forbidden** | **normal** }

undo mvrp registration

View

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

Default level

2: System level

Parameters

fixed: Specifies the fixed registration mode.

forbidden: Specifies the forbidden registration mode.

normal: Specifies the normal registration mode.

Description

Use **mvrp registration** to set the MVRP registration mode on the port.

Use **undo mvrp registration** to restore the default.

By default, the MVRP registration mode is normal.

This command is available only on trunk ports.

Related commands: **display mvrp running-status**.

Examples

# Configure GigabitEthernet 1/0/1 as a trunk port, and set the MVRP registration mode to fixed on the port.

```
<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 all
[Sysname-GigabitEthernet1/0/1] mvrp registration fixed
```

reset mvrp statistics

Syntax

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

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, the command clears MVRP statistics of all ports.

Description

Use **reset mvrp statistics** to clear the MVRP statistics of ports.

Related commands: **display mvrp statistics**.

Examples

# Clear the MVRP statistics of all ports.

```
<Sysname> reset mvrp statistics
```

Index

Contents

ARP configuration commands

arp check enable

Syntax

arp check enable

undo arp check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp check enable** to enable dynamic ARP entry check.

Use **undo arp check enable** to disable dynamic ARP entry check.

By default, dynamic ARP entry check is enabled.

Examples

# Enable dynamic ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

View

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

Default level

2: System level

Parameters

number: Specifies the maximum number of dynamic ARP entries that an interface can learn, in the range of 0 to 1024.

Description

Use **arp max-learning-num** to configure the maximum number of dynamic ARP entries that an interface can learn.

Use **undo arp max-learning-num** to restore the default.

By default, a Layer 2 interface does not limit the number of dynamic ARP entries. The maximum number of dynamic ARP entries that a Layer 3 interface can learn is 1024.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

# Specify VLAN-interface 40 to learn up to 50 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 50
```

# Specify GigabitEthernet 1/0/1 to learn up to 100 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 100
```

# Specify Layer 2 aggregate interface bridge-aggregation 1 to learn up to 100 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 100
```

arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address in an ARP entry.

mac-address: Specifies the MAC address in an ARP entry, in the format H-H-H.

vlan-id: Specifies the ID of a VLAN to which a static ARP entry belongs, in the range of 1 to 4094.

interface-type interface-number: Specifies the interface type and interface number.

Description

Use **arp static** to configure a static ARP entry in the ARP mapping table.

Use **undo arp** to remove an ARP entry.

A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if long, will be deleted, and if short and resolved, will become unresolved.

The *vlan-id* argument specifies the VLAN corresponding to an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interface following the argument must belong to that VLAN. The VLAN interface of the VLAN must have been created.

If both the *vlan-id* and *ip-address* arguments are specified, the IP address of the VLAN interface corresponding to the *vlan-id* argument must be in the same network segment as the IP address specified by the *ip-address* argument.

Related commands: **reset arp** and **display arp**.

Examples

# Configure a static ARP entry, with IP address 202.38.10.2, MAC address 00e0-fc01-0000, and outbound interface GigabitEthernet 1/0/1 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 GigabitEthernet 1/0/1
```

arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Default level

2: System level

Parameters

aging-time: Specifies the age timer for dynamic ARP entries in minutes, ranging from 1 to 1440.

Description

Use **arp timer aging** to set the age timer for dynamic ARP entries.

Use **undo arp timer aging** to restore the default.

By default, the age timer for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

Examples

# Set the age timer for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

display arp

Syntax

display arp [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Displays the ARP entries on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4094.

interface *interface-type interface-number:* Displays the ARP entries of the interface specified by the argument *interface-type interface-number*.

count: Displays the number of ARP entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp** to display ARP entries in the ARP mapping table.

If no parameter is specified, all ARP entries are displayed.

Related commands: **arp static** and **reset arp**.

Examples

# Display the information of all ARP entries.

```
<Sysname> display arp all
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface              Aging Type
192.168.0.235    00e0-fc02-2181  1        GE1/0/30               20    D
192.168.0.86     00e0-fc00-7801  1        GE1/0/30               9     D
192.168.0.161    000f-e000-0003  1        GE1/0/30               20    D
192.168.0.162    00e0-fc14-000b  1        GE1/0/30               20    D
```

Table 1 Command output

Field	Description
IP Address	IP address in an ARP entry.
MAC Address	MAC address in an ARP entry.
VLAN ID	ID of the VLAN that the ARP entry belongs to.
Interface	Outbound interface in an ARP entry.
Aging	Aging time for a dynamic ARP entry in minutes (**DIS** or **N/A** means unknown aging time or no aging time).

Field	Description
Type	ARP entry type: - **D**—Dynamic. - **S**—Static.

# Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total Entry(ies):  4
```

display arp *ip-address*

Syntax

display arp *ip-address* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Displays the ARP entries on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp** *ip-address* to display the ARP entry for a specified IP address.

Related commands: **arp static** and **reset arp**.

Examples

# Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface              Aging Type
20.1.1.1         00e0-fc00-0001  N/A      N/A                    N/A   S
```

display arp timer aging

Syntax

display arp timer aging [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp timer aging** to display the age timer for dynamic ARP entries.

Related commands: **arp timer aging**.

Examples

# Display the age timer for dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 10 minute(s)
```

mac-address station-move

Syntax

mac-address station-move quick-notify enable

undo mac-address station-move quick-notify enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **mac-address station-move quick-notify enable** to enable ARP quick update.

Use **undo mac-address station-move quick-notify enable** to restore the default.

By default, ARP quick update is disabled.

Example

# Enable ARP quick update.

```
<Sysname> system-view
[Sysname] mac-address station-move quick-notify enable
```

reset arp

Syntax

reset arp { **all** | **dynamic** | **static** | **slot** *slot-number* | **interface** *interface-type interface-number* }

View

User view

Default level

2: System level

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Clears the ARP entries on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

interface *interface-type interface-number*: Clears the ARP entries for the interface specified by the argument *interface-type interface-number*.

Description

Use **reset arp** to clear ARP entries from the ARP mapping table.

With **interface** *interface-type interface-number* specified, the command clears only dynamic ARP entries of the interface.

Related commands: **arp static** and **display arp**.

Examples

# Clear all static ARP entries.

```
<Sysname> reset arp static
```

Gratuitous ARP configuration commands

arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *milliseconds*]

undo arp send-gratuitous-arp

View

VLAN interface view

Default level

2: System level

Parameters

interval *milliseconds*: Sets the interval at which gratuitous ARP packets are sent, in the range of 200 to 200,000 milliseconds. The default value is 2000.

Description

Use **arp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets and set the sending interval for the interface.

Use **undo arp send-gratuitous-arp** to disable the interface from periodically sending gratuitous ARP packets.

By default, an interface is disabled from sending gratuitous ARP packets periodically.

This function takes effect only when the link of the enabled interface goes up and an IP address has been assigned to the interface.

If you change the interval for sending gratuitous ARP packets, the configuration is effective at the next sending interval.

The frequency of sending gratuitous ARP packets may be much lower than is expected if this function is enabled on multiple interfaces, or each interface is configured with multiple secondary IP addresses, or 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-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **gratuitous-arp-sending enable** to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use **undo gratuitous-arp-sending enable** to restore the default.

By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Examples

# Disable a device from sending gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **gratuitous-arp-learning enable** to enable the gratuitous ARP packet learning function.

Use **undo gratuitous-arp-learning enable** to disable the function.

By default, the function is enabled.

With this function enabled, a device receiving a gratuitous ARP packet can add the source IP and MAC addresses to its own dynamic ARP table if it finds that no ARP entry exists in the cache corresponding to the source IP address of the ARP packet. If a matching ARP entry is found in the cache, the device updates the ARP entry regardless of whether this function is enabled.

Examples

# Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

Proxy ARP configuration commands

display local-proxy-arp

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Displays the local proxy ARP status of the interface specified by the argument *interface-type interface-number*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display local-proxy-arp** to display the status of the local proxy ARP.

If no interface is specified, the local proxy ARP status of all interfaces is displayed.

Related commands: **local-proxy-arp enable**.

Examples

# Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

display proxy-arp

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Displays the proxy ARP status of the interface specified by the argument *interface-type interface-number*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display proxy-arp** to display the proxy ARP status.

If an interface is specified, the proxy ARP status of the specified interface is displayed; if no interface is specified, the proxy ARP status of all interfaces is displayed.

Related commands: **proxy-arp enable**.

Examples

# Display the proxy ARP status on VLAN-interface 1.

```
<Sysname> display proxy-arp interface Vlan-interface 1
Interface Vlan-interface 1
 Proxy ARP status: disabled
```

local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *startIP* **to** *endIP*]

undo local-proxy-arp enable

View

VLAN interface view

Default level

2: System level

Parameters

ip-range *startIP* **to** *endIP*: 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.

Description

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

By default, local proxy ARP is disabled.

Only one IP address range can be specified by using the **ip-range** keyword on an interface.

Related commands: **display local-proxy-arp**.

Examples

# Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

# Enable local proxy ARP on VLAN-interface 2 for a specific 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
```

proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

View

VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

By default, proxy ARP is disabled.

Related commands: **display proxy-arp**.

Examples

# Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

ARP snooping configuration commands

arp-snooping enable

Syntax

arp-snooping enable

undo arp-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **arp-snooping enable** to enable ARP snooping.

Use **undo arp-snooping enable** to disable ARP snooping.

By default, ARP snooping is disabled.

Examples

# Enable ARP snooping on VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp-snooping enable
```

display arp-snooping

Syntax

display arp-snooping [**ip** *ip-address* | **vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

ip *ip-address*: Displays the ARP snooping entry information for the IP address.

vlan *vlan-id*: Displays ARP snooping entries of a specified VLAN. The *vlan-id* argument is in the range of 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp-snooping** to display ARP snooping entries. If no keywords or arguments are specified, the command displays all the ARP snooping entries.

Examples

# Display ARP snooping entries of VLAN 1.

```
<Sysname> display arp-snooping vlan 1
IP Address   MAC Address    VLAN ID Interface  Aging       Status
3.3.3.3      0003-0003-0003 1       GE1/0/1     20          Valid
3.3.3.4      0004-0004-0004 1       GE1/0/2     5           Invalid
---- Total entry(ies) on VLAN 1:2 ----
```

reset arp-snooping

Syntax

reset arp-snooping [**ip** *ip-address* | **vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

ip *ip-address*: Removes the ARP entry of a specified IP address.

vlan *vlan-id*: Removes the ARP entries of a specified VLAN. The *vlan-id* argument is in the range of 1 to 4094.

Description

Use **reset arp-snooping** to remove ARP snooping entries. If no keywords or arguments are specified, the command removes all ARP snooping entries.

Examples

# Remove ARP snooping entries of VLAN 1.

```
<Sysname> reset arp-snooping vlan 1
```

IP addressing configuration commands

display ip interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip interface** to display IP configuration information for a specified Layer 3 interface or all Layer 3 interfaces.

Examples

# Display IP configuration information for interface VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state :DOWN
Line protocol current state :DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
```

```
Source quench:                0
Routing redirect:             0
Echo request:                 0
Router advert:                0
Router solicit:               0
Time exceed:                  0
IP header bad:                0
Timestamp request:            0
Timestamp reply:              0
Information request:          0
Information reply:            0
Netmask request:              0
Netmask reply:                0
Unknown type:                 0
```

Table 2 Command output

Field	Description
current state	Current physical state of the interface: • **Administrative DOWN**—The interface is shut down with the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • **UP**—Both the administrative and physical states of the interface are up.
Line protocol current state	Current state of the link layer protocol, which can be: • **DOWN**—The protocol state of the interface is down. • **UP**—The protocol state of the interface is up. • **UP (spoofing)**—The protocol state of the interface pretends to be up; however, no corresponding link is present, or the corresponding link is not present permanently but is established as needed.
Internet Address	IP address of an interface: • **Primary**—Identifies a primary IP address. • **Sub**—Identifies a secondary IP address. • **acquired via DHCP**—Identifies an IP address obtained through DHCP. • **acquired via BOOTP**—Identifies an IP address obtained through BOOTP. • **Cluster**—Identifies a cluster IP address. • **Mad**—Identifies a MAD IP address.
Broadcast address	Broadcast address of the subnet attached to an interface.
The Maximum Transmit Unit	Maximum transmission units on the interface, in bytes.
input packets, bytes, multicasts output packets, bytes, multicasts	Unicast packets, bytes, and multicast packets received on an interface (the statistics start at the device startup).

Field	Description
ARP packet input number: Request packet: Reply packet: Unknown packet:	Total number of ARP packets received on the interface (the statistics start at the device startup), including: • ARP request packets • ARP reply packets • Unknown packets
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the device startup).
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (the statistics start at the device startup), including: • 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. • Timestamp request packets. • Timestamp reply packets. • Information request packets. • Information reply packets. • Netmask request packets. • Netmask reply packets. • Unknown type packets.

display ip interface brief

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip interface brief** to display brief IP configuration information for a specified Layer 3 interface or all Layer 3 interfaces.

- Without the interface type and interface number specified, the brief IP configuration information for all Layer 3 interfaces is displayed.
- With only the interface type specified, the brief IP configuration information for all Layer 3 interfaces of the specified type is displayed.
- With both the interface type and interface number specified, only the brief IP configuration information for the specified interface is displayed.

Related commands: **display ip interface**.

Examples

# Display brief IP configuration information for VLAN interfaces.

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing
Interface           Physical Protocol IP Address      Description
Vlan1                up       up       6.6.6.6         Vlan-inte...
Vlan2                up       up       7.7.7.7         Vlan-inte...
```

Table 3 Command output

Field	Description
*down: administratively down	The interface is administratively shut down with the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. It indicates that an interface may have no link present even when its link layer protocol is displayed **up** or the link is set up only on demand.
Interface	Interface name.
Physical	Physical state of the interface: • ***down**—The interface is administratively down; that is, the interface is shut down with the **shutdown** command. • **down**—The interface is administratively up but its physical state is down. • **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. • **up**—That the protocol state of the interface is up. • **up(s)**—The protocol state of the interface is up (spoofing).
IP Address	IP address of the interface (If no IP address is configured, **unassigned** is displayed.)
Description	Interface description information, for which up to 12 characters can be displayed. If there are more than 12 characters, only the first nine characters are displayed.

ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]]

View

Interface view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of an interface, in dotted decimal notation.

mask-length: Specifies the subnet mask length, the number of consecutive ones in the mask.

mask: Specifies the subnet mask in dotted decimal notation.

sub: Specifies the secondary IP address for the interface.

Description

Use **ip address** to assign an IP address and mask to the interface.

Use **undo ip address** to remove all IP addresses from the interface.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to remove a secondary IP address.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You cannot assign a secondary IP address to the interface that is configured to obtain one through BOOTP or DHCP.

Related commands: **display ip interface**.

Examples

# Assign VLAN-interface 1 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

DHCP server configuration commands

bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** | **simple**] *key*

undo bims-server

View

DHCP address pool view

Default level

2: System level

Parameters

ip *ip-address*: Specifies an IP address for the BIMS server.

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

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Description

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

Use **undo bims-server** to remove the specified BIMS server information.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

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

bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

View

DHCP address pool view

Default level

2: System level

Parameters

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

Description

Use **bootfile-name** to specify a bootfile name in the DHCP address pool for the client.

Use **undo bootfile-name** to remove the specified bootfile name.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the bootfile name **aaa.cfg** in DHCP address pool 0.

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

dhcp dscp (for DHCP server)

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

View

System view

Default level

2: System level

Parameters

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

Description

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

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

By default, the DSCP value in DHCP packets sent by the DHCP server is 56.

Examples

# Set the DSCP value to 30 for DHCP packets.

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

dhcp enable

Syntax

dhcp enable

undo dhcp enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp enable** to enable DHCP.

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

By default, DHCP is disabled.

You need to enable DHCP before performing DHCP server and relay agent configurations.

Examples

# Enable DHCP.

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

dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool [*pool-name*]

View

Interface view

Default level

2: System level

Parameters

pool-name: DHCP address pool name, a case-insensitive string in the range of 1 to 35 characters.

Description

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

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

By default, no extended address pool is applied on an interface, and the server assigns an IP address from a common address pool to a client when the client's request arrives at the interface.

- If you execute the **dhcp server apply ip-pool** command on an interface, when a client's request arrives at the interface, the server attempts to assign the client the statically bound IP address first and then an IP address from this extended address pool.
- Only an extended address pool can be applied on an interface. The address pool to be referenced must already exist.

Related commands: **dhcp server ip-pool**.

Examples

# Apply extended DHCP address pool 0 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp server apply ip-pool 0
```

dhcp select server global-pool

Syntax

dhcp select server global-pool [**subaddress**]

undo dhcp select server global-pool [**subaddress**]

View

Interface view

Default level

2: System level

Parameters

subaddress: Supports secondary address allocation. When the DHCP server and client are on the same network segment, the server preferably assigns an IP address from an address pool that resides on the same subnet as the primary IP address of the server interface (connecting to the client). If the address pool contains no assignable IP address, the server assigns an IP address from an address pool that resides on the same subnet as the secondary IP addresses of the server interface. If the interface has multiple secondary IP addresses, each address pool is tried in turn for address allocation. Without the keyword **subaddress** specified, the DHCP server can only assign an IP address from the address pool that resides on the same subnet as the primary IP address of the server interface.

Description

Use **dhcp select server global-pool** to enable the DHCP server on specified interface(s). After the interface receives a DHCP request from a client, the DHCP server will allocate an IP address from the address pool.

Use **undo dhcp select server global-pool** to remove the configuration. Upon receiving a DHCP request from a client, the interface will neither assign an IP address to the client, nor serve as a DHCP relay agent to forward the request.

Use the **undo dhcp select server global-pool subaddress** command to disable the support for secondary address allocation.

By default, the DHCP server is enabled on an interface.

Examples

# Enable the DHCP server on VLAN-interface 1 to assign IP addresses from the address pool that resides on the same subnet as the primary IP address of the server interface (connecting to the client) for the client.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select server global-pool
```

dhcp server client-detect enable

Syntax

dhcp server client-detect enable

undo dhcp server client-detect enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp server client-detect enable** to enable client off-line detection on the DHCP server.

Use **undo dhcp server client-detect enable** to disable the function.

By default, the function is disabled.

With this feature enabled, the DHCP server considers a DHCP client goes offline when the ARP entry for the client ages out. In addition, it removes the client's IP-to-MAC binding entry.

Examples

# Enable client off-line detection on the DHCP server.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp server client-detect enable
```

dhcp server detect

Syntax

dhcp server detect

undo dhcp server detect

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp server detect** to enable unauthorized DHCP server detection.

Use **undo dhcp server detect** to disable the function.

By default, the function is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP server resolves from the request the IP addresses of DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can use this information to check for unauthorized DHCP servers.

Examples

# Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

View

System view

Default level

2: System level

Parameters

low-ip-address: Specifies the start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: Specifies the end IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description

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

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

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.

When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified with the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify the same address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.

Using the **dhcp server forbidden-ip** command repeatedly can exclude multiple IP address ranges from allocation.

Related commands: **display dhcp server forbidden-ip**, **dhcp server ip-pool**, **network**, and **static-bind ip-address**.

Examples

# Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

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

dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name* [**extended**]

undo dhcp server ip-pool *pool-name*

View

System view

Default level

2: System level

Parameters

pool-name: Specifies the global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

extended: Specifies the address pool as an extended address pool. If this keyword is not specified, the address pool is a common address pool.

Description

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

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

By default, no DHCP address pool is created.

Related commands: **dhcp enable** and **display dhcp server tree**.

Examples

# Create the common address pool identified by 0.

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

dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

View

System view

Default level

2: System level

Parameters

number: Specifies the number of ping packets, in the range of 0 to 10. 0 means no ping operation.

Description

Use **dhcp server ping packets** to specify the maximum number of ping packets on the DHCP server.

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

The number defaults to 1.

To avoid IP address conflicts, the DHCP server checks whether an IP address is in use before assigning it to a DHCP client.

The DHCP server pings the IP address to be assigned by using ICMP. If the server gets a response within the specified period, the server selects and pings another IP address. If not, the server pings the IP address again until the specified number of ping attempts is reached. If still no response is received, the server assigns the IP address to the requesting client.

Examples

# Specify the maximum number of ping packets as 10.

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

dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

View

System view

Default level

2: System level

Parameters

milliseconds: Specifies the response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. 0 means no ping operation.

Description

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

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

The time defaults to 500 ms.

To avoid IP address conflicts, the DHCP server checks whether an IP address is in use before assigning it to a DHCP client.

The DHCP server pings the IP address to be assigned by using ICMP. If the server gets a response within the specified interval, the server selects and pings another IP address. If not, the server pings the IP address again until the specified number of ping attempts is reached. If still no response is received, the server assigns the IP address to the requesting client.

Examples

# Specify the response timeout time as 1000 ms.

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

dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **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.

By default, the DHCP server handles Option 82.

Examples

# Configure the DHCP server to ignore Option 82.

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

dhcp server threshold

Syntax

dhcp server threshold { **allocated-ip** *threshold-value* | **average-ip-use** *threshold-value* | **max-ip-use** *threshold-value* }

undo dhcp server threshold { **allocated-ip** | **average-ip-use** | **max-ip-use** }

View

System view

Default level

2: System level

Parameters

allocated-ip *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the ratio of successfully allocated IP addresses to received DHCP requests within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

average-ip-use *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the average IP address utilization of an address pool within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

max-ip-use *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the maximum IP address utilization of an address pool within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

Description

Use **dhcp server threshold** to enable the DHCP server to send trap messages to the network management server when the specified threshold is reached.

Use **undo dhcp server threshold** to restore the default.

By default, the DHCP server does not send trap messages to the network management server.

Examples

# Enable the DHCP server to send trap messages to the network management server when the ratio of successfully allocated IP addresses to received DHCP requests within five minutes exceeds 50%.

```
<Sysname> system-view
[Sysname] dhcp server threshold allocated-ip 50
```

# Enable the DHCP server to send trap messages to the network management server when the average IP address utilization of an address pool within five minutes exceeds 80%.

```
<Sysname> system-view
[Sysname] dhcp server threshold average-ip-use 80
```

# Enable the DHCP server to send trap messages to the network management server when the maximum IP address utilization of an address pool within five minutes exceeds 80%.

```
<Sysname> system-view
[Sysname] dhcp server threshold max-ip-use 80
```

display dhcp server conflict

Syntax

display dhcp server conflict { **all** | **ip** *ip-address* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information about all IP address conflicts.

ip-address: Displays conflict information for a specified IP address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Related commands: **reset dhcp server conflict**.

Examples

# Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
    Address             Discover time
    4.4.4.1             Apr 25 2007 16:57:20
    4.4.4.2             Apr 25 2007 17:00:10
 --- total 2 entry ---
```

Table 4 Command output

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

display dhcp server expired

Syntax

display dhcp server expired { **all** | **ip** *ip-address* | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the lease expiration information of all DHCP address pools.

ip *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server expired** to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Examples

# Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
 IP address       Client-identifier/    Lease expiration          Type
                    Hardware address
 4.4.4.6          3030-3066-2e65-3230-  Apr 25 2007 17:10:47     Release
                   302e-3130-3234-2d45-
                   7468-6572-6e65-7430-
                   2f31

 --- total 1 entry ---
```

Table 5 Command output

Field	Description
IP address	Expired IP addresses.
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired.
Lease expiration	The lease expiration time.
Type	Types of lease expirations. This field is set to **Release**.

display dhcp server free-ip

Syntax

display dhcp server free-ip [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server free-ip** to display information about assignable IP addresses which have never been assigned.

Examples

# Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.1              to  10.0.0.254
```

display dhcp server forbidden-ip

Syntax

display dhcp server forbidden-ip [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server forbidden-ip** to display IP addresses excluded from dynamic allocation in DHCP address pool.

Examples

# Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
Global:
IP Range from 1.1.0.2              to  1.1.0.3
IP Range from 1.1.1.2              to  1.1.1.3
Pool name: 2
1.1.1.5          1.1.1.6
```

Table 6 Command output

Field	Description
Global	Globally excluded IP addresses specified with the **dhcp server forbidden-ip** command in system view. No address pool can assign these IP addresses.

Field	Description
Pool name	Excluded IP addresses specified with the **forbidden-ip** command in DHCP address pool view. They cannot be assigned from the current extended address pool only.

display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the binding information of all DHCP address pools.

ip *ip-address*: Displays the binding information of a specified IP address.

pool [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server ip-in-use** to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use**.

Examples

# Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
Pool utilization: 0.39%
 IP address     Client-identifier/    Lease expiration        Type
                   Hardware address
 10.1.1.1        4444-4444-4444        NOT Used                  Manual
 10.1.1.2       3030-3030-2e30-3030-   May  1 2009 14:02:49      Auto:COMMITTED
                662e-3030-3033-2d45-
                7468-6572-6e65-7430-
                2f31
```

```
--- total 2 entry ---
```

Table 7 Command output

Field	Description
Pool utilization	Utilization rate of IP addresses in a DHCP address pool, which is the ratio of assigned IP addresses to assignable IP addresses in the DHCP address pool. • When the binding information of all DHCP address pools is displayed, this field displays the total utilization rate of IP addresses in all DHCP address pools. • When the binding information of a specific DHCP address pool is displayed, this field displays the utilization rate of IP addresses in the DHCP address pool. • When the binding information of a specific IP address is displayed, this field is not displayed.
IP address	Bound IP address.
Client-identifier/Hardware address	Client's ID or MAC of the binding.
Lease expiration	Lease expiration time: • **Specific time (May 1 2009 14:02:49 in this example)**—Time when the lease expires. • **NOT Used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time.
Type	Binding types: • **Manual**—Static binding. • **Auto:OFFERED**—The binding sent in the DHCP-OFFER message from the server to the client. • **Auto:COMMITTED**—The binding sent in the DHCP-ACK message from the server to the client.

display dhcp server statistics

Syntax

display dhcp server statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Related commands: **reset dhcp server statistics**.

Examples

# Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
    Global Pool:
      Pool Number:                     1
      Binding:
        Auto:                          1
        Manual:                        0
        Expire:                        0
    BOOTP Request:                     10
      DHCPDISCOVER:                    5
      DHCPREQUEST:                     3
      DHCPDECLINE:                     0
      DHCPRELEASE:                     2
      DHCPINFORM:                      0
      BOOTPREQUEST:                    0
    BOOTP Reply:                       6
      DHCPOFFER:                       3
      DHCPACK:                         3
      DHCPNAK:                         0
      BOOTPREPLY:                      0
    Bad Messages:                      0
```

Table 8 Command output

Field	Description
Global Pool	Statistics of a DHCP address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings
Manual	The number of static bindings
Expire	The number of expired bindings
BOOTP Request	The number of DHCP requests sent from DHCP clients to the DHCP server. The requests include: • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREQUEST

Field	Description
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients. The replies include: • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY
Bad Messages	The number of Erroneous messages

display dhcp server tree

Syntax

display dhcp server tree { **all** | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information of all DHCP address pools.

pool [*pool-name*]: Displays information of a specified address pool. The *pool name* argument is a string of 1 to 35 characters. If no *pool name* is specified, information of all address pools will be displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server tree** to display information of DHCP address pool(s).

Examples

# Display information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:

Pool name: 0
 network 20.1.1.0 mask 255.255.255.0
 Sibling node:1
 option 2 ip-address 1.1.1.1
 expired 1 0 0 0

Pool name: 1
```

```
 static-bind ip-address 10.10.1.2 mask 255.0.0.0
 static-bind mac-address 00e0-00fc-0001
 PrevSibling node:0
 expired unlimited

Extended pool:

Pool name: 2
 network ip range 1.1.1.0 1.1.1.255
 network mask 255.255.255.0
 expired 0 0 2 0
```

Table 9 Command output

Field	Description
Global pool	Information of a common address pool.
Pool name	Address pool name.
network	Subnet for address allocation.
static-bind ip-address 10.10.1.2 mask 255.0.0.0 static-bind mac-address 00e0-00fc-0001	The IP address and MAC address of the static binding.
Sibling node	The sibling node of the current node. Nodes of this kind in the output can be: • **Child node**—The child node (subnet segment) address pool of the current node • **Parent node**—The parent node (nature network segment) address pool of the current node • **Sibling node**—The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher order the sibling node has. • **PrevSibling node**—The previous sibling node of the current node
option	Self-defined DHCP options.
expired	The lease duration, in the format of day, hour, minute, and second.
Extended pool	Information of an extended address pool.
network ip range	Range of assignable IP addresses in the extended address pool.
network mask	Mask of IP addresses assigned from the extended address pool.

dns-list

Syntax

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

undo dns-list { *ip-address* | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Specifies the DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to be removed.

Description

Use **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.

By default, no DNS server address is specified.

If you perform the **dns-list** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP address pool 0.

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

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCP address pool view

Default level

2: System level

Parameters

domain-name: Domain name suffix for DHCP clients, a string of 1 to 50 characters.

Description

Use **domain-name** to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use **undo domain-name** to remove the specified domain name suffix.

No domain name suffix is specified by default.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify a domain name suffix of mydomain.com for the DHCP clients in DHCP address pool 0.

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

```
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax

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

undo expired

View

DHCP address pool view

Default level

2: System level

Parameters

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

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

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

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

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

Description

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

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

By default, the lease duration of a static address pool is unlimited, and the lease duration of a dynamic address pool is one day.

The lease duration cannot be less than 5 seconds.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the lease duration as one day, two hours, three minutes, and four 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
```

forbidden-ip

Syntax

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

undo forbidden-ip { *ip-address*&<1-8> | **all** }

View

DHCP extended address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Specifies the IP addresses to be excluded from dynamic allocation. &<1-8> indicates that you can specify up to eight IP addresses, separated with spaces.

all: Excludes all IP addresses from dynamic allocation.

Description

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

Use **undo forbidden-ip** to cancel specified or all excluded IP addresses.

By default, all IP addresses in an extended address pool are assignable except the IP addresses of the DHCP server interfaces.

- Only the extended address pools support this command.
- IP addresses specified with the **forbidden-ip** command in DHCP address pool view are excluded from dynamic address allocation in the current extended address pool only. They are assignable in other address pools.
- Repeatedly using the **forbidden-ip** command can exclude multiple IP address ranges from dynamic allocation.

Related commands: **dhcp server ip-pool** and **display dhcp server forbidden-ip**.

Examples

# Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation for extended address pool 0.

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

gateway-list

Syntax

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

undo gateway-list { *ip-address* | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Specifies the gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description

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

Use **undo gateway-list** to remove specified gateway addresses specified for the DHCP client from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the gateway address 10.110.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax

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

undo nbns-list { *ip-address* | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Specifies the WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **netbios-type**, and **display dhcp server tree**.

Examples

# Specify WINS server address 10.12.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View

DHCP address pool view

Default level

2: System level

Parameters

b-node: 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, and if receiving no response, then broadcasts it to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name, and if receiving no response, then 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.

Description

Use **netbios-type** to specify the client NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to remove the specified client NetBIOS node type.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool**, **nbns-list**, and **display dhcp server tree**.

Examples

# Specify the NetBIOS node type as b-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network

View

DHCP address pool view

Default level

2: System level

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length and 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 IP address network mask, in dotted decimal format.

Description

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

No subnet is specified by default.

You can specify only one subnet for each common address pool. If you use the **network** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify 192.168.8.0/24 as the subnet for dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

network ip range

Syntax

network ip range *min-address max-address*

undo network ip range

View

DHCP address pool view

Default level

2: System level

Parameters

min-address: Specifies the lowest IP address for dynamic allocation.

max-address: Specifies the highest IP address for dynamic allocation.

Description

Use **network ip range** to specify the IP address range for dynamic allocation in an address pool.

Use **undo network ip range** to remove the specified address range.

No IP address range is specified by default.

In a common address pool, you can use the **network ip range** command to further specify an IP address range on a subnet for address allocation. The specified IP address range must belong to the subnet; otherwise the common address pool cannot assign IP addresses.

You can specify only one IP address range for each address pool. If you use the **network ip range** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **network**, and **display dhcp server tree**.

Examples

# Specify addresses 10.1.1.1 through 10.1.1.150 on subnet 10.1.1.0/24 for dynamic address allocation in common address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
```

```
[Sysname-dhcp-pool-1] network 10.1.1.0 24
[Sysname-dhcp-pool-1] network ip range 10.1.1.1 10.1.1.150
```

# Specify addresses 192.168.8.1 through 192.168.8.150 for dynamic address allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network ip range 192.168.8.1 192.168.8.150
```

network mask

Syntax

network mask *mask*

undo network mask

View

DHCP extended address pool view

Default level

2: System level

Parameters

mask: Specifies a network mask, in dotted decimal notation.

Description

Use **network mask** to specify the IP address mask for dynamic allocation in an extended address pool.

Use **undo network mask** to remove the specified IP address mask.

No IP address mask is specified by default.

Only the extended address pools support this command.

If you specify an IP address range for an extended address pool without an IP address mask, the extended address pool is not valid, and therefore the system cannot assign IP addresses from the extended address pool.

Related commands: **dhcp server ip-pool**, **display dhcp server tree**, and **network ip range**.

Examples

# Specify 255.255.255.0 as the IP address mask for dynamic allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network mask 255.255.255.0
```

next-server

Syntax

next-server *ip-address*

undo next-server

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a server.

Description

Use **next-server** to specify the IP address of a server for DHCP clients.

Use **undo next-server** to remove the server's IP address from the DHCP address pool.

By default, no server's IP address is specified in the address pool on the DHCP server.

If you repeatedly execute this command, the new configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify a server's IP address 1.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 1.1.1.1
```

option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View

DHCP address pool view

Default level

2: System level

Parameters

code: Self-defined option number, in the range of 2 to 254, excluding 12, 50 to 55, 57 to 61, and 82.

ascii *ascii-string*: Specifies an ASCII string with 1 to 255 characters.

hex *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates that you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates that you can specify up to eight IP addresses, separated by spaces.

Description

Use **option** to configure a self-defined DHCP option in a DHCP address pool.

Use **undo option** to remove a self-defined DHCP option from a DHCP address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Configure the hex digits 0x11 and 0x22 for the self-defined DHCP Option 100 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax

reset dhcp server conflict { **all** | **ip** *ip-address* }

View

User view

Default level

2: System level

Parameters

all: Clears the statistics of all IP address conflicts.

ip *ip-address*: Clears the conflict statistics of a specified IP address.

Description

Use **reset dhcp server conflict** to clear statistics of IP address conflict(s).

Related commands: **display dhcp server conflict**.

Examples

# Clears the statistics of all IP address conflicts.

```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View

User view

Default level

2: System level

Parameters

all: Clears the IP address dynamic binding information of all DHCP address pools.

ip *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description

Use **reset dhcp server ip-in-use** to clear dynamic IP address binding information.

Related commands: **display dhcp server ip-in-use**.

Examples

# Clear the binding information of IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset dhcp server statistics** to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics**.

Examples

# Clear the statistics of the DHCP server.

```
<Sysname> reset dhcp server statistics
```

static-bind client-identifier

Syntax

static-bind client-identifier *client-identifier*

undo static-bind client-identifier

View

DHCP address pool view

Default level

2: System level

Parameters

client-identifier: Client ID of a static binding, a string with 4 to 160 characters in the format of H-H-H…, each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, but aabb-c-dddd and aabb-cc-dddd are both invalid.

Description

Use **static-bind client-identifier** to specify the client ID of a static binding in a DHCP address pool.

Use **undo static-bind client-identifier** to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **static-bind ip-address**, **static-bind mac-address**, **display dhcp server tree**, and **display dhcp client verbose**.

Examples

# Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a static binding. If no mask and mask length is specified, the natural mask is used.

mask-length: Specifies the mask length of the IP address, which is the number of 1s in the mask, in the range of 1 to 30.

mask *mask*: Specifies the IP address mask, in dotted decimal format.

Description

Use **static-bind ip-address** to specify an IP address in a DHCP address pool for a static binding.

Use **undo static-bind ip-address** to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- The IP address of the static binding cannot be an interface address of the DHCP server. Otherwise, an IP address conflict may occur, and the bound client cannot obtain an IP address correctly.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind mac-address**, and **display dhcp server tree**.

Examples

# Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax

static-bind mac-address *mac-address*

undo static-bind mac-address

View

DHCP address pool view

Default level

2: System level

Parameters

mac-address: Specifies the MAC address of a static binding, in the format of H-H-H.

Description

Use **static-bind mac-address** to statically bind a MAC address to an IP address in a DHCP address pool.

Use **undo static-bind mac-address** to remove the statically bound MAC address.

By default, no MAC address is statically bound.

Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.

If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration overwrites the previous one.

Relate commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind ip-address**, **display dhcp server tree**.

Examples

# Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

View

DHCP address pool view

Default level

2: System level

Parameters

domain-name: Specifies the TFTP server name, a string of 1 to 63 characters.

Description

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

Use **undo tftp-server domain-name** to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

If you perform the **tftp-server domain-name** command repeatedly, the last configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the TFTP server name as aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: Specifies the TFTP server IP address.

Description

Use **tftp-server ip-address** to specify the TFTP server IP address in a DHCP address pool.

Use **undo tftp-server ip-address** to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

If you perform the **tftp-server ip-address** command repeatedly, the last configuration overwrites the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

vendor-class-identifier

Syntax

vendor-class-identifier *hex-string*&<1-255> **ip range** *min-address max-address*

undo vendor-class-identifier *hex-string*&<1-255>

View

DHCP extended address pool view

Default level

2: System level

Parameters

hex-string&<1-255>: A character string, which is used to match against Option 60 (vendor class identifier option). *hex-string* is a hexadecimal number ranging from 0 to FF. &<1-255> indicates that you can type up to 255 hexadecimal numbers, which are separated by spaces.

ip range *min-address max-address*: Specifies the IP address range for dynamic allocation. *min-address* is the lowest IP address and *max-address* is the highest IP address for dynamic allocation.

Description

Use **vendor-class-identifier** to specify an IP address range for the DHCP clients of a specified vendor.

Use **undo vendor-class-identifier** to restore the default.

By default, no IP address range is specified for the DHCP clients of any vendor.

After this feature is configured in an extended DHCP address pool, the DHCP server, when using the extended DHCP address pool to assign an IP address to a DHCP client, checks whether Option 60 in the DHCP request is the same as the character string configured with the **vendor-class-identifier** command. If yes, the DHCP server selects an IP address from the address range specified with this command. If not, the DHCP server selects one from the address range specified with the **network ip range** command.

NOTE:

- Only extended address pools support this command.
- The IP address range specified with this command must be included in that specified with the **network ip range** command.

Related commands: **network ip range** and **network mask**.

Examples

# Specify IP address rang 10.1.1.1 to 10.1.1.5 for the DHCP clients of vender a0 b0 0c.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] vendor-class-identifier a0 b0 0c ip range 10.1.1.1 10.1.1.5
```

voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

View

DHCP address pool view

Default level

2: System level

Parameters

as-ip *ip-address*: Specifies the IP address for the backup network calling processor. When the primary network calling processor is unavailable, the DHCP client uses the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and "*".

ncp-ip *ip-address*: Specifies the IP address for the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

disable: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.

enable: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

Description

Use **voice-config** to configure specified Option 184 contents in a DHCP address pool.

Use **undo voice-config** to remove specified Option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

You must specify the IP address of a network calling processor first to make other configured parameters take effect.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

# Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

DHCP relay agent configuration commands

The DHCP relay agent configuration is supported only VLAN interfaces.

dhcp dscp (for DHCP relay agent)

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

View

System view

Default level

2: System level

Parameters

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

Description

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

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

By default, the DSCP value in DHCP packets sent by the DHCP relay agent is 56.

Examples

# Set the DSCP value to 30 for DHCP packets.

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

dhcp relay address-check enable

Syntax

dhcp relay address-check enable

undo dhcp relay address-check enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp relay address-check enable** to enable address check on the relay agent.

Use **undo dhcp relay address-check enable** to disable address check on the relay agent.

By default, the function is disabled.

With this feature enabled, the DHCP relay agent can dynamically record clients' IP-to-MAC bindings after clients get IP addresses through DHCP. It also supports static bindings. You can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external networks using fixed IP addresses.

Upon receiving an ARP packet, the DHCP relay agent matches the sender's IP and MAC addresses in the packet against the bindings (both dynamic and static). If no match is found, the DHCP relay agent does not learn the ARP entry. The sending host cannot access external networks via the DHCP relay agent.

This command can be executed only on VLAN interfaces.

The **dhcp relay address-check enable** command only checks IP and MAC addresses of clients.

Examples

# Enable address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

dhcp relay check mac-address

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp relay check mac-address** to enable MAC address check on the DHCP relay agent.

Use **undo dhcp relay check mac-address** to disable MAC address check on the DHCP relay agent.

By default, this function is disabled.

With this function enabled, the DHCP relay agent compares the chaddr field of a received DHCP request with the source MAC address field of the frame. If they are the same, the DHCP relay agent decides this request as valid and forwards it to the DHCP server; if not, the DHCP request is discarded.

DHCP relay agents change the source MAC addresses when forwarding DHCP packets. Therefore, you can enable MAC address check only on a DHCP relay agent directly connected to the DHCP clients. Otherwise, valid DHCP packets may be discarded and clients cannot obtain IP addresses.

Examples

# Enable MAC address check on the DHCP relay agent.

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

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay check mac-address
```

dhcp relay client-detect enable

Syntax

dhcp relay client-detect enable

undo dhcp relay client-detect enable

View

Interface view

Default level

2: System level

Parameters

None

Description

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

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

By default, this function is disabled.

With this function enabled on an interface, the DHCP relay agent removes a client's IP-to-MAC binding entry when it is aged out, and sends a DHCP-RELEASE request to the DHCP server to release the IP address of the client.

Examples

# Enable offline detection on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay client-detect enable
```

dhcp relay information circuit-id format-type

Syntax

dhcp relay information circuit-id format-type { **ascii** | **hex** }

undo dhcp relay information circuit-id format-type

View

Interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use **dhcp relay information circuit-id format-type** to configure the code type for the non-user-defined circuit ID sub-option.

Use **undo dhcp relay information circuit-id format-type** to restore the default.

By default, the code type for the circuit ID sub-option depends on the specified padding format of Option 82. Each field has its own code type.

This command applies only to configuring the non-user-defined circuit ID sub-option. After you configure the padding content for the circuit ID sub-option using the **dhcp relay information circuit-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp relay information**.

Examples

# Configure the code type for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id format-type ascii
```

dhcp relay information circuit-id string

Syntax

dhcp relay information circuit-id string *circuit-id*

undo dhcp relay information circuit-id string

View

Interface view

Default level

2: System level

Parameters

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use **dhcp relay information circuit-id string** to configure the padding content for the user-defined circuit ID sub-option.

Use **undo dhcp relay information circuit-id string** to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format** and **display dhcp relay information**.

Examples

# Configure the padding content for the circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] dhcp relay information circuit-id string company001
```

dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp relay information enable** to enable the relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

By default, Option 82 support is disabled on the DHCP relay agent.

Related commands: **display dhcp relay information**.

Examples

# Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
```

dhcp relay information format

Syntax

dhcp relay information format { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format

View

Interface view

Default level

2: System level

Parameters

normal: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using the MAC address as the node identifier.

- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description

Use **dhcp relay information format** to specify a padding format for Option 82.

Use **undo dhcp relay information format** to restore the default padding format.

The Option 82 padding format defaults to **normal**.

If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.

If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.

Related commands: **display dhcp relay information**.

Examples

# Specify the verbose padding format for Option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy replace
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

dhcp relay information remote-id format-type

Syntax

dhcp relay information remote-id format-type { **ascii** | **hex** }

undo dhcp relay information remote-id format-type

View

Interface view

Default level

2: System view

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use **dhcp relay information remote-id format-type** to configure the code type for the non-user-defined remote ID sub-option.

Use **undo dhcp relay information remote-id format-type** to restore the default.

By default, the code type for the remote ID sub-option is HEX.

This command applies only to configuring the non-user-defined remote ID sub-option. After you configure the padding content for the remote ID sub-option using the **dhcp relay information remote-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp relay information**.

Examples

# Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id format-type ascii
```

dhcp relay information remote-id string

Syntax

dhcp relay information remote-id string { *remote-id* | **sysname** }

undo dhcp relay information remote-id string

View

Interface view

Default level

2: System level

Parameters

remote-id: Padding content for the user-defined remote ID sub-option, a case-sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use **dhcp relay information remote-id string** to configure the padding content for the user-defined remote ID sub-option.

Use **undo dhcp relay information remote-id string** to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string** "Sysname" command.

Related commands: **dhcp relay information format** and **display dhcp relay information**.

Examples

# Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id string device001
```

dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View

Interface view

Default level

2: System level

Parameters

drop: Specifies the dropping of messages containing Option 82.

keep: Specifies the forwarding of messages containing Option 82 without any change.

replace: Specifies the forwarding of messages containing Option 82 after replacing the original Option 82 with the Option 82 padded in the specified padding format.

Description

Use **dhcp relay information strategy** to configure DHCP relay agent handling strategy for messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

The handling strategy for messages containing Option 82 defaults to **replace**.

Related commands: **display dhcp relay information**.

Examples

# Configure the DHCP relay agent handling strategy for messages containing Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

dhcp relay release ip

Syntax

dhcp relay release ip *client-ip*

View

System view

Default level

2: System level

Parameters

client-ip: Specifies the DHCP client IP address.

Description

Use **dhcp relay release ip** to request the DHCP server to release a specified client IP address.

Examples

# Request the DHCP server to release the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax

dhcp relay security static *ip-address mac-address* [**interface** *interface-type interface-number*]

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the client IP address for creating a static binding.

mac-address: Specifies the client MAC address for creating a static binding, in the format H-H-H.

interface *interface-type interface-number*: Specifies a Layer 3 interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

all: Specifies that all client entries are to be removed.

dynamic: Specifies that dynamic client entries are to be removed.

static: Specifies that manual client entries are to be removed.

Description

Use **dhcp relay security static** to configure a static client entry, which is the binding between IP address, MAC address, and Layer 3 interface on the relay agent.

Use **undo dhcp relay security** to remove specified client entries from the relay agent.

No manual client entry is configured on the DHCP relay agent by default.

- When using the **dhcp relay security static** command to bind an interface to a static client entry, make sure that the interface is configured as a DHCP relay agent; otherwise, entry conflicts may occur.
- The **undo dhcp relay security interface** command is used to remove all the dynamic client entries from the interface.

Related commands: **display dhcp relay security**.

Examples

# Bind DHCP relay interface VLAN-interface 2 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 10.10.1.1 0005-5d02-f2b3 interface vlan-interface
2
```

dhcp relay security refresh enable

Syntax

dhcp relay security refresh enable

undo dhcp relay security refresh enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp relay security refresh enable** to enable the DHCP relay agent to periodically refresh dynamic client entries.

Use **undo dhcp relay security refresh enable** to disable periodic refresh of dynamic client entries.

By default, the DHCP relay agent is enabled to periodically refresh dynamic client entries.

If you disable the DHCP relay agent from periodically refreshing dynamic client entries, such entries do not age automatically. Therefore, if a client relinquishes its IP address, you need to manually remove the corresponding dynamic client entry on the DHCP relay agent.

Related commands: **dhcp relay security tracker** and **dhcp relay security static**.

Examples

# Disable the DHCP relay agent from periodically refreshing dynamic client entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay security refresh enable
```

dhcp relay security tracker

Syntax

dhcp relay security tracker { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View

System view

Default level

2: System level

Parameters

interval: Specifies the refreshing interval in seconds, in the range of 1 to 120.

auto: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. The more entries there are, the shorter the interval. The shortest interval is no less than 500 ms.

Description

Use **dhcp relay security tracker** to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use **undo dhcp relay security tracker** to restore the default interval.

The default refreshing interval is **auto**, the value of 60 seconds divided by the number of binding entries.

Related commands: **display dhcp relay security tracker**.

Examples

# Set the refreshing interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax

dhcp relay server-detect

undo dhcp relay server-detect

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp relay server-detect** to enable unauthorized DHCP server detection.

Use **undo dhcp relay server-detect** to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP relay agent will record from the request the IP addresses of all DHCP servers that ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can use this information from logs to check for unauthorized DHCP servers.

After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.

Examples

# Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax

dhcp relay server-group *group-id* **ip** *ip-address*

undo dhcp relay server-group *group-id* [**ip** *ip-address*]

View

System view

Default level

2: System level

Parameters

group-id: Specifies a DHCP server group by its number, in the range of 0 to 19.

ip *ip-address*: Specifies a DHCP server IP address.

Description

Use **dhcp relay server-group** to specify a DHCP server for a DHCP server group.

Use **undo dhcp relay server-group** to remove a DHCP server from a DHCP server group, if no **ip** *ip-address* is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

- The IP address of a DHCP server and the IP address of the DHCP relay agent's interface that connects the DHCP client cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.
- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related commands: **display dhcp relay server-group**.

Examples

# Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax

dhcp relay server-select *group-id*

undo dhcp relay server-select

View

Interface view

Default level

2: System level

Parameters

group-id: Specifies a DHCP server group by its number to be correlated, in the range of 0 to 19.

Description

Use **dhcp relay server-select** to correlate specified interfaces to a specified DHCP server group.

Use **undo dhcp relay server-select** to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

- A DHCP server group can correlate with one or multiple DHCP relay agent interfaces.
- A relay agent interface can only correlate with one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.
- The DHCP server group referenced in this command should have been configured by using the **dhcp relay server-group** command.

Related commands: **dhcp relay server-group** and **display dhcp relay**.

Examples

# Correlate VLAN-interface 1 to DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

dhcp select relay

Syntax

dhcp select relay

undo dhcp select relay

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp select relay** to enable the relay agent on the current interface. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use **undo dhcp select relay** to restore the default.

After DHCP is enabled, the DHCP server is enabled on an interface by default. Upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

When the operating mode of the interface is changed from DHCP server to DHCP relay agent, the IP address leases will not be deleted. To avoid this, delete the existing IP address leases when changing the interface operating mode to DHCP relay agent.

Examples

# Enable the DHCP relay agent on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

display dhcp relay

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information of DHCP server groups that all interfaces correspond to.

interface *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay** to display information about DHCP server groups correlated to an interface or all interfaces.

Examples

# Display information about DHCP server groups correlated to all interfaces.

```
<Sysname> display dhcp relay all
    Interface name            Server-group
    Vlan-interface1                   2
```

Table 10 Command output

Field	Description
Server-group	DHCP server group number correlated to the interface

display dhcp relay information

Syntax

display dhcp relay information { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all interfaces.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay information** to display Option 82 configuration information on the DHCP relay agent.

Examples

# Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp relay information all
Interface: Vlan-interface100
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: aabbcc
    User defined:
         Circuit ID: company001
Interface: Vlan-interface200
    Status: Enable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
         Remote ID: device001
```

Table 11 Command output

Field	Description
Interface	Interface name.
Status	Option 82 state, which can be **Enable** or **Disable**.
Strategy	Handling strategy for requesting messages containing Option 82, which can be **Drop**, **Keep**, or **Replace**.
Format	Padding format of Option 82, which can be **Normal** or **Verbose**.

Field	Description
Circuit ID format-type	Non-user-defined code type of the circuit ID sub-option, which can be **ASCII** or **HEX**.
Remote ID format-type	Non-user-defined code type of the remote ID sub-option, which can be **ASCII** or **HEX**.
Node identifier	Access node identifier.
User defined	Content of user-defined sub-options.
Circuit ID	User-defined padding content of the circuit ID sub-option.
Remote ID	User-defined padding content of the remote ID sub-option.

display dhcp relay security

Syntax

display dhcp relay security [*ip-address* | **dynamic** | **static**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Displays the binding information of an IP address.

dynamic: Displays information about dynamic bindings.

static: Displays information about static bindings.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay security** to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

You must enable address check, or IP source guard on the DHCP relay agent before it can generate dynamic client entries. For more information about IP source guard, see *Security Configuration Guide*.

Examples

# Display information about all bindings.

```
<Sysname> display dhcp relay security
IP Address       MAC Address      Type       Interface
 10.1.1.5        00e0-0000-0000   Static     Vlan2
```

```
---   1 dhcp-security item(s) found   ---
```

Table 12 Command output

Field	Description
IP Address	Client IP address.
MAC Address	Client MAC address.
Type	Type of binding, including dynamic, static, and temporary.
Interface	Layer 3 interface connecting to the DHCP client. If no interface is recorded in the binding entry, **N/A** is displayed.

display dhcp relay security statistics

Syntax

display dhcp relay security statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay security statistics** to display statistics about bindings of DHCP relay agents.

You must enable address check, or IP source guard on the DHCP relay agent before it can generate dynamic client entries. For more information about IP source guard, see *Security Configuration Guide*.

Examples

# Display statistics about bindings of DHCP relay agents.

```
<Sysname> display dhcp relay security statistics
Static Items      :1
Dynamic Items     :0
Temporary Items   :0
All Items         :1
```

Table 13 Command output

Field	Description
Static Items	Static binding items

Field	Description
Dynamic Items	Dynamic binding items
Temporary Items	Temporary binding items
All Items	All binding items

display dhcp relay security tracker

Syntax

display dhcp relay security tracker [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay security tracker** to display the interval for refreshing dynamic bindings on the relay agent.

Examples

# Display the interval for refreshing dynamic bindings on the relay agent.

```
<Sysname> display dhcp relay security tracker
 Current tracker interval : 10s
```

The interval is 10 seconds.

display dhcp relay server-group

Syntax

display dhcp relay server-group { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Displays the information of the specified DHCP server group numbered from 0 to 19.

all: Displays the information of all DHCP server groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay server-group** to display the configuration information of a specified DHCP server group or all DHCP server groups.

Examples

# Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
    No.            Group IP
    1              1.1.1.1
    2              1.1.1.2
```

Table 14 Command output

Field	Description
No.	Sequence number
Group IP	IP address in the server group

display dhcp relay statistics

Syntax

display dhcp relay statistics [**server-group** { *group-id* | **all** }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Specifies a server group by its number, in the range of 0 to 19, about display DHCP packet statistics is to be displayed.

all: Specifies all server groups about which DHCP packet statistics is to be displayed. Information for each group is displayed independently.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay statistics** to display DHCP packet statistics related to a specified DHCP server group or all DHCP server groups.

If no parameter (**server-group** and **all)** is specified, all DHCP packet statistics on the relay agent will be displayed.

Related commands: **reset dhcp relay statistics**.

Examples

# Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
     Bad packets received:                    0
     DHCP packets received from clients:      0
         DHCPDISCOVER packets received:       0
         DHCPREQUEST packets received:        0
         DHCPINFORM packets received:         0
         DHCPRELEASE packets received:        0
         DHCPDECLINE packets received:        0
         BOOTPREQUEST packets received:       0
     DHCP packets received from servers:      0
         DHCPOFFER packets received:          0
         DHCPACK packets received:            0
         DHCPNAK packets received:            0
         BOOTPREPLY packets received:         0
     DHCP packets relayed to servers:         0
         DHCPDISCOVER packets relayed:        0
         DHCPREQUEST packets relayed:         0
         DHCPINFORM packets relayed:          0
         DHCPRELEASE packets relayed:         0
         DHCPDECLINE packets relayed:         0
         BOOTPREQUEST packets relayed:        0
     DHCP packets relayed to clients:         0
         DHCPOFFER packets relayed:           0
         DHCPACK packets relayed:             0
         DHCPNAK packets relayed:             0
         BOOTPREPLY packets relayed:          0
     DHCP packets sent to servers:            0
         DHCPDISCOVER packets sent:           0
         DHCPREQUEST packets sent:            0
         DHCPINFORM packets sent:             0
         DHCPRELEASE packets sent:            0
         DHCPDECLINE packets sent:            0
         BOOTPREQUEST packets sent:           0
     DHCP packets sent to clients:            0
         DHCPOFFER packets sent:              0
         DHCPACK packets sent:                0
         DHCPNAK packets sent:                0
         BOOTPREPLY packets sent:             0
```

# Display DHCP packet statistics related to every server group on the relay agent.

```
<Sysname> display dhcp relay statistics server-group all
DHCP relay server-group           #0
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                 0
     DHCPREQUEST                  0
     DHCPINFORM                   0
     DHCPRELEASE                  0
     DHCPDECLINE                  0
     BOOTPREQUEST                 0
 Server -> Client:
     DHCPOFFER                    0
     DHCPACK                      0
     DHCPNAK                      0
     BOOTPREPLY                   0
```

reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**server-group** *group-id*]

View

User view

Default level

1: Monitor level

Parameters

server-group *group-id*: Specifies a server group by its number, in the range of 0 to 19, about which statistics is to be removed from the relay agent.

Description

Use **reset dhcp relay statistics** to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related commands: **display dhcp relay statistics**.

Examples

# Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```

DHCP client configuration commands

The DHCP client configuration is supported only on VLAN interfaces.

When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows Server 2000 or Windows Server 2003.

display dhcp client

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

verbose: Specifies verbose DHCP client information to be displayed.

interface *interface-type interface-number*: Specifies an interface for which to display DHCP client information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp client** to display DHCP client information. If no **interface** *interface-type interface-number* is specified, DHCP client information of all interfaces will be displayed.

Examples

# Display DHCP client information of all interfaces.

```
<Sysname> display dhcp client
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

# Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from 2005.08.13 15:37:59   to   2005.08.16 15:37:59
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static route:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS server: 44.1.1.11
 DNS server: 44.1.1.12
 Domain name: ddd.com
 Boot server: 200.200.200.200  1.1.1.1
 Client ID: 3030-3066-2e65-3234-
            392e-3830-3438-2d56-
            6c61-6e2d-696e-7465-
            7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 15 Command output

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client.
Current machine state	Current state of the DHCP client: • **HALT**—Indicates that the client stops applying for an IP address. • **INIT**—Indicates the initialization state. • **SELECTING**—Indicates that the client has sent out a DHCP-DISCOVER message in search of a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—Indicates that the client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—Indicates that the client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—Indicates that the T1 timer expires. • **REBOUNDING**—Indicates that the T2 timer expires.
Allocated IP	The IP address allocated by the DHCP server.
Allocated lease	The allocated lease time.
T1	The 1/2 lease time (in seconds) of the DHCP client IP address.
T2	The 7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address.
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client.

Field	Description
Classless static route	Classless static routes assigned to the client.
Static route	Classful static routes assigned to the client.
DNS server	The DNS server address assigned to the client.
Domain name	The domain name suffix assigned to the client.
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID.
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long until the T1 (1/2 lease time) timer times out.

dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

View

System view

Default level

2: System level

Parameters

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

Description

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.

By default, the DSCP value in DHCP packets sent by the DHCP client is 56.

Examples

# Set the DSCP value to 30 for DHCP packets.

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

ip address dhcp-alloc

Syntax

ip address dhcp-alloc [**client-identifier mac** *interface-type interface-number*]

undo ip address dhcp-alloc

View

Interface view

Default level

2: System level

Parameters

client-identifier mac *interface-type interface-number*: Specifies the MAC address of an interface to be used as the client ID to obtain an IP address.

Description

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.

By default, an interface does not use DHCP for IP address acquisition.

If no parameter is specified, the client uses a character string that comprises the current interface name and MAC address as its ID for address acquisition.

The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.

Examples

# Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```

DHCP snooping configuration commands

A DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server. It can work when it is between the DHCP client and relay agent or between the DHCP client and server.

dhcp-snooping

Syntax

dhcp-snooping

undo dhcp-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping** to enable DHCP snooping.

Use **undo dhcp-snooping** to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

Related commands: **display dhcp-snooping**.

Examples

# Enable DHCP snooping.

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

dhcp-snooping binding database filename

Syntax

dhcp-snooping binding database filename *filename*

undo dhcp-snooping binding database filename

View

System view

Default level

2: System level

Parameters

filename: File name. For how to define the file name, see *Fundamentals Configuration Guide*.

Description

Use **dhcp-snooping binding database filename** to specify the name of the file for storing DHCP snooping entries.

Use **undo dhcp-snooping binding database filename** to restore the default.

By default, no file name is specified.

If no file with the specified name is found, the device will automatically create the file upon storing a DHCP snooping binding.

DHCP snooping entries are stored immediately after this command is used, and then updated at the interval set by the **dhcp-snooping binding database update interval** command.

Related commands: **dhcp-snooping binding database update interval**.

Examples

# Specify the name of the file for storing DHCP snooping entries as **database.dhcp**.

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

dhcp-snooping binding database update interval

Syntax

dhcp-snooping binding database update interval *minutes*

undo dhcp-snooping binding database update interval

View

System view

Default level

2: System level

Parameters

minutes: Specifies the refresh interval in minutes, in the range of 1 to 14400.

Description

Use **dhcp-snooping binding database update interval** to set the interval at which the DHCP snooping entry file is refreshed.

Use **undo dhcp-snooping binding database update interval** to restore the default.

By default, the DHCP snooping entry file is not refreshed periodically.

With this command configured, DHCP snooping will check bindings periodically. If a binding is added or removed during an interval, DHCP snooping will add or remove this binding to or from the file at the end of this interval; if no change occurs within the interval, DHCP snooping will not refresh the file.

This command takes effect only when the DHCP snooping entry file is specified.

Related commands: **dhcp-snooping binding database filename**.

Examples

# Configure the DHCP snooping entry file to be refreshed every 10 minutes.

```
<Sysname> system-view
[Sysname] dhcp-snoooping binding database update interval 10
```

dhcp-snooping binding database update now

Syntax

dhcp-snooping binding database update now

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping binding database update now** to store DHCP snooping entries to the file.

DHCP snooping entries will be stored to the file each time this command is used.

This command takes effect only when the DHCP snooping entry file is specified.

Related commands: **dhcp-snooping binding database filename**.

Examples

# Store DHCP snooping entries to the file.

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

dhcp-snooping check mac-address

Syntax

dhcp-snooping check mac-address

undo dhcp-snooping check mac-address

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping check mac-address** to enable MAC address check on a DHCP snooping device.

Use **undo dhcp-snooping check mac-address** to disable MAC address check of DHCP snooping.

By default, this function is disabled.

With this function enabled, the DHCP snooping device compares the chaddr field of a received DHCP request with the source MAC address field in the frame. If they are the same, the DHCP snooping device decides this request valid and forwards it to the DHCP server. If not, the DHCP request is discarded.

Examples

# Enable MAC address check of DHCP snooping.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping check mac-address
```

dhcp-snooping check request-message

Syntax

dhcp-snooping check request-message

undo dhcp-snooping check request-message

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping check request-message** to enable DHCP-REQUEST message check of DHCP snooping.

Use **undo dhcp-snooping check request-message** to disable DHCP-REQUEST message check of the DHCP snooping.

By default, this function is disabled.

With this function enabled, upon receiving a DHCP-REQUEST message, a DHCP snooping device searches local DHCP snooping entries for the corresponding entry of the message. If an entry is found, the DHCP snooping device compares the entry with the message information. If they are consistent, the DHCP-REQUEST message is considered as valid lease renewal request and forwarded to the DHCP server. If they are not consistent, the messages is considered as forged lease renewal request and discarded. If no corresponding entry is found locally, the message is considered valid and forwarded to the DHCP server.

Examples

# Enable DHCP-REQUEST message check of DHCP snooping.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping check request-message
```

dhcp-snooping information circuit-id format-type

Syntax

dhcp-snooping information circuit-id format-type { **ascii** | **hex** }

undo dhcp-snooping information circuit-id format-type

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use **dhcp-snooping information circuit-id format-type** to configure the code type for the non-user-defined circuit ID sub-option.

Use **undo dhcp-snooping information circuit-id format-type** to restore the default.

By default, the code type for the circuit ID sub-option depends on the padding format of Option 82. Each field has its own code type.

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp-snooping information circuit-id string** command, ASCII is adopted as the code type. The private padding format supports only the hex code type.

Related commands: **display dhcp-snooping information** and **dhcp-snooping information format.**

Examples

# Configure the padding format for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id format-type ascii
```

dhcp-snooping information circuit-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string** *circuit-id*

undo dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string**

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

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

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use **dhcp-snooping information circuit-id string** to configure the padding content for the user-defined circuit ID sub-option.

Use **undo dhcp-snooping information circuit-id string** to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

- After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured circuit ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured circuit ID sub-option takes effect in all VLANs. The former case has a higher priority. The circuit ID sub-option specified for a VLAN will be padded for packets within the VLAN.

Related commands: **dhcp-snooping information format** and **display dhcp-snooping information**.

Examples

# Configure the padding content for the user-defined circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id string company001
```

dhcp-snooping information enable

Syntax

dhcp-snooping information enable

undo dhcp-snooping information enable

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping information enable** to configure DHCP snooping to support Option 82.

Use **undo dhcp-snooping information enable** to disable this function.

By default, DHCP snooping does not support Option 82.

Related commands: **display dhcp-snooping information**.

Examples

# Configure DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
```

dhcp-snooping information format

Syntax

dhcp-snooping information format { **normal** | **private** *private* | **standard** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp-snooping information format

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

normal: Specifies the normal padding format.

private *private*: Specifies the private padding format. The *private* value can only be 1, which represents the private padding format.

standard: Specifies the standard padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string of 1 to 50 characters.

Description

Use **dhcp-snooping information format** to specify the padding format for Option 82.

Use **undo dhcp-snooping information format** to restore the default.

By default, the padding format for Option 82 is **normal**.

When you use the **undo dhcp-snooping information format** command, if the **verbose node-identifier** argument is not specified, the padding format will be restored to **normal**; if the **verbose node-identifier** argument is specified, the padding format will be restored to **verbose** with MAC address as the node identifier.

Related commands: **display dhcp-snooping information**.

Examples

# Specify the padding format as **verbose** for Option 82.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information format verbose
```

dhcp-snooping information remote-id format-type

Syntax

dhcp-snooping information remote-id format-type { **ascii** | **hex** }

undo dhcp-snooping information remote-id format-type

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use **dhcp-snooping information remote-id format-type** to configure the code type for the non-user-defined remote ID sub-option.

Use **undo dhcp-snooping information remote-id format-type** to restore the default.

By default, the code type for the remote ID sub-option is HEX.

This command applies to configuring a non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp-snooping information remote-id string** command, ASCII is adopted as the code type. The private padding format only supports the hex code type.

Related commands: **display dhcp-snooping information** and **dhcp-snooping information format**.

Examples

# Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id format-type ascii
```

dhcp-snooping information remote-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **remote-id string** { *remote-id* | **sysname** }

undo dhcp-snooping information [**vlan** *vlan-id*] **remote-id string**

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

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

remote-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use **dhcp-snooping information remote-id string** to configure the padding content for the user-defined remote ID sub-option.

Use **undo dhcp-snooping information remote-id string** to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

- After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured remote ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured remote ID sub-option takes effect in all VLANs. The former case has a higher priority. The remote ID sub-option configured for a VLAN will be padded for the packets within the VLAN.

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp-snooping information remote-id string** "Sysname" command.

Related commands: **dhcp-snooping information format** and **display dhcp-snooping information**.

Examples

# Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id string device001
```

dhcp-snooping information strategy

Syntax

dhcp-snooping information strategy { **append** |**drop** | **keep** | **replace** }

undo dhcp-snooping information strategy

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

append: Forwards the message containing Option 82 after adding content to the sub-option 9 of option 82. The append strategy is supported only when the private padding format and sub-option 9 are configured. In other cases, the device forwards the message without changing Option 82.

drop: Drops the message containing Option 82.

keep: Forwards the message containing Option 82 without changing Option 82.

replace: Forwards the message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

Description

Use **dhcp-snooping information strategy** to configure the handling strategy for Option 82 in requesting messages.

Use **undo dhcp-snooping information strategy** to restore the default.

By default, the handling strategy for Option 82 in requesting messages is **replace**.

Related commands: **display dhcp-snooping information**, **dhcp-snooping information format** and **dhcp-snooping information sub-option.**

Examples

# Configure the handling strategy for Option 82 in requesting messages as **keep**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy keep
```

dhcp-snooping information sub-option

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **sub-option** *sub-option-code* [**string** *user-string*&<1-8>]

undo dhcp-snooping information [**vlan** *vlan-id*] **sub-option** *sub-option-code*

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

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

sub-option *sub-option-code*: Specifies the number of the sub-option. Currently, only sub-option 9 is supported.

string *user-string*&<1-8>: Configures the content of the sub-option, a case-sensitive string of 1 to 63 characters. &<1-8> represents that you can enter a maximum of 8 strings separated by spaces.

Description

Use **dhcp-snooping information sub-option** to configure a sub-option.

Use **undo dhcp-snooping information sub-option** to restore the default.

By default, no sub-option is configured.

This configuration applies to the private padding format only. To configure the private padding format, use the **dhcp-snooping information format private 1** command.

If no content is configured for sub-option 9 with the **string** *user-string* option, the primary device uses sysname and the primary address of the Loopback0 interface to pad sub-option 9 and the secondary device uses sysname to pad sub-option 9. The device configured with the **dhcp-snooping information**

strategy append command is the primary device and a device configured with some other strategy is a secondary device.

After you use the **string** *user-string* option to configure sub-option 9, the device uses the ASCII code type to pad the characters into sub-option 9 in the order that they are configured. When the total length of all sub-options reaches 255, the device stops padding automatically.

The sub-option 9 content configured only applies to the VLAN that is specified by the **vlan** *vlan-id* option. If no VLAN ID is specified, the sub-option 9 content applies to all VLANs. A VLAN prefers its own sub-option 9 content over the one configured for all VLANs.

Related commands: **dhcp-snooping information format**, **dhcp-snooping information strategy**, and **display dhcp-snooping information**.

Examples

# Configure the user-defined sub-option 9 as group001.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] dhcp-snooping information sub-option 9 string group001
```

dhcp-snooping rate-limit

Syntax

dhcp-snooping rate-limit *rate*

undo dhcp-snooping rate-limit

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

rate: Maximum rate of incoming DHCP packets, ranging from 64 to 512 Kbps.

Description

Use **dhcp-snooping rate-limit** to configure the maximum rate of incoming DHCP packets.

Use **undo dhcp-snooping rate-limit** to restore the default.

By default, DHCP packet rate limit is disabled.

This command takes effect only after you enable DHCP snooping.

An interface configured with DHCP packet rate limit discards incoming DHCP packets exceeding the specified maximum rate.

If a Layer 2 Ethernet port belongs to an aggregation group, it uses the DHCP packet maximum rate configured on the corresponding Layer 2 aggregate interface.

Examples

# Set the maximum rate of incoming DHCP packets on Layer 2 Ethernet port GigabitEthernet 1/0/1 to 64 Kbps.

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

```
[Sysname-GigabitEthernet1/0/1] dhcp-snooping rate-limit 64
```

dhcp-snooping trust

Syntax

dhcp-snooping trust [**no-user-binding**]

undo dhcp-snooping trust

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

no-user-binding: Specifies the port not to record the clients' IP-to-MAC bindings in DHCP requests it receives. The command without this keyword records the IP-to-MAC bindings of clients.

Description

Use **dhcp-snooping trust** to configure a port as a trusted port.

Use **undo dhcp-snooping trust** to restore the default state of a port.

All ports are untrusted by default.

After enabling DHCP snooping, you need to specify the ports connected to the valid DHCP servers as trusted to make sure that DHCP clients can obtain valid IP addresses.

Related commands: **display dhcp-snooping trust**.

Examples

# Specify GigabitEthernet 1/0/1 as a trusted port and enable it to record the IP-to-MAC bindings of clients.

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

display dhcp-snooping

Syntax

display dhcp-snooping [**ip** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip *ip-address*: Displays the DHCP snooping entries corresponding to the specified IP address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping** to display DHCP snooping entries.

Only the DHCP snooping entries containing IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages are displayed by using the **display dhcp-snooping** command.

Related commands: **dhcp-snooping** and **reset dhcp-snooping**.

Examples

# Display all DHCP snooping entries.

```
<Sysname> display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== =============== ============== ============ ==== ===== =================
 D    10.1.1.1        00e0-fc00-0006 286          1    2     GigabitEthernet1/0/1
---   1 dhcp-snooping item(s) found   ---
```

Table 16 Command output

Field	Description
Type	Entry type: - **D**—Dynamic. - **S**—Static. Static DHCP snooping entries are not supported. - **R**—The DHCP snooping entry is being restored through the DHCP snooping entry file, and the interface in the entry is invalid.
IP Address	IP address assigned to the DHCP client.
MAC Address	MAC address of the DHCP client.
Lease	Lease period left (in seconds).
VLAN	Outer VLAN tag when DHCP snooping and QinQ are both enabled or the DHCP snooping device receives a packet with two VLAN tags; or VLAN where the port connecting the DHCP client resides.
SVLAN	Inner VLAN tag when DHCP snooping and QinQ are both enabled or the DHCP snooping device receives a packet with two VLAN tags; or N/A.
Interface	Port to which the DHCP client is connected.

display dhcp-snooping binding database

Syntax

display dhcp-snooping binding database [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping binding database** to display the DHCP snooping entry file information.

Examples

# Display the DHCP snooping entry file information.

```
<Sysname> display dhcp-snooping binding database
File name                     :   flash:/database.dhcp
Update interval               :   10 minutes
Latest read time              :   Jul 15 2008 16:38:22
Latest write time             :   Jul 15 2008 16:38:24
Status                        :   Last write succeeded.
```

Table 17 Command output

Field	Description
File name	File name.
Update interval	Interval at which the DHCP snooping entry file is refreshed.
Latest read time	Last time when the file is read.
Latest write time	Last time when the file is written.
Status	Indicates whether the file was written successfully last time.

display dhcp-snooping information

Syntax

display dhcp-snooping information { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all Layer 2 Ethernet ports.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping information** to display Option 82 configuration information on the DHCP snooping device.

Examples

# Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp-snooping information all
Interface: GigabitEthernet 1/0/1
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: aabbcc
    Sub-option 9: Enabled
    User defined:
        Circuit ID: company001
        Sub-option 9 content: group1
Interface: GigabitEthernet 1/0/2
    Status: Disable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
        Circuit ID: company001
        Remote ID: device001
        VLAN 10:
            Circuit ID: vlan10@company001
            Sub-option 9: Enable
            Sub-option 9 content: group1
        VLAN 20:
            Remote ID: device001
           Sub-option 9: Enabled
```

display dhcp-snooping packet statistics

Syntax

display dhcp-snooping packet statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the DHCP packet statistics of a specified IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters

Description

Use **display dhcp-snooping packet statistics** to display DHCP packet statistics on the DHCP snooping device.

Related commands: **reset dhcp-snooping packet statistics**.

Examples

# Display DHCP packet statistics on the DHCP snooping device.

```
<Sysname> display dhcp-snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Packets dropped due to rate limitation : 20
 Dropped invalid packets                : 0
```

display dhcp-snooping trust

Syntax

display dhcp-snooping trust [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping trust** to display information about trusted ports.

Related commands: **dhcp-snooping trust**.

Examples

# Display information about trusted ports.

```
<Sysname> display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                        Trusted
 =========================                     ============
 GigabitEthernet1/0/1                              Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabitEthernet 1/0/1 is trusted.

reset dhcp-snooping

Syntax

reset dhcp-snooping { **all** | **ip** *ip-address* }

View

User view

Default level

2: System level

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entries of the specified IP address.

Description

Use **reset dhcp-snooping** to clear DHCP snooping entries.

Related commands: **display dhcp-snooping**.

Examples

# Clear all DHCP snooping entries.

```
<Sysname> reset dhcp-snooping all
```

reset dhcp-snooping packet statistics

Syntax

reset dhcp-snooping packet statistics [**slot** *slot-number*]

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the DHCP packet statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset dhcp-snooping packet statistics** to clear DHCP packet statistics on the DHCP snooping device.

Related commands: **display dhcp-snooping packet statistics**.

Examples

# Clear DHCP packet statistics on the DHCP snooping device.

```
<Sysname> reset dhcp-snooping packet statistics
```

BOOTP client configuration commands

BOOTP client configuration can only be used on VLAN interfaces.

If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows Server 2000 or Windows Server 2003.

display bootp client

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the BOOTP client information of the interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bootp client** to display related information about a BOOTP client.

- If **interface** *interface-type interface-number* is not specified, the command will display information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command will display information about the BOOTP client on the specified interface.

Examples

# Display related information of the BOOTP client on VLAN-interface 1.

```
<Sysname> display bootp client interface vlan-interface 1
Vlan-interface1 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

Table 18 Command output

Field	Description
Vlan-interface1 BOOTP client information	Information of the interface serving as a BOOTP client.
Allocated IP	IP address assigned to the BOOTP client.
Transaction ID	Value of the **XID** field in a BOOTP message, which is a random number chosen when the BOOTP client sends a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client will drop the BOOTP response.
Mac Address	MAC address of a BOOTP client.

ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ip address bootp-alloc** to enable an interface to obtain an IP address through BOOTP.

Use **undo ip address bootp-alloc** to disable the interface from obtaining an IP address through BOOTP.

By default, an interface does not obtain an IP address through BOOTP.

Related commands: **display bootp client**.

Examples

# Configure VLAN-interface 1 to obtain IP address through the BOOTP protocol.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address bootp-alloc
```

IPv4 DNS configuration commands

display dns domain

Syntax

display dns domain [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns domain** to display the domain name suffixes.

Related commands: **dns domain**.

Examples

# Display domain name suffixes.

```
<Sysname> display dns domain
 Type:
  D:Dynamic    S:Static

No.    Type   Domain-name
1      S      com
```

Table 19 Command output

Field	Description
No	Sequence number.
Type	Type of domain name suffix: **S** represents a statically configured domain name suffix, and **D** represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix.

display dns host

Syntax

display dns host [**ip** | **ipv6** | **naptr** | **srv**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip: Displays the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Displays the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Displays the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Displays the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns host** to display the dynamic DNS cache information.

Without any keyword specified, the dynamic DNS cache information of all query types will be displayed.

Related commands: **reset dns host**.

Examples

# Display the dynamic DNS cache information of all query types.

```
<Sysname> display dns host
No.  Host                       TTL  Type  Reply Data
1    sample.com                 3132 IP    192.168.10.1
2    sample.net                 2925 IPv6  FE80::4904:4448
3    sip.sample.com             3122 NAPTR 100 10 u sip+E2U !^.*$!sip:info.se!i
4    website.tcp.sample.com     3029 SRV   10 10 8080 iis.sample.com
```

Table 20 Command output

Field	Description
No	Sequence number.

Field	Description
Host	Domain name for query.
TTL	Time that a mapping can be stored in the cache (in seconds).
Type	Query type, including IP, IPv6, NAPTR, and SRV.
Reply Data	Reply data concerning the query type: • For an IP query, the reply data is an IPv4 address. • For an IPv6 query, the reply data is an IPv6 address. • For a NAPTR query, the reply data comprises order, preference, flags, services, regular expression, and replacement. • For an SRV query, the reply data comprises the priority, weight, port, and target domain name.

display dns server

Syntax

display dns server [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays the DNS server information dynamically obtained through DHCP or other protocols

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns server** to display the IPv4 DNS server information.

Related commands: **dns server**.

Examples

# Display the IPv4 DNS server information.

```
<Sysname> display dns server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IP Address
    1       S     169.254.65.125
```

Table 21 Command output

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: **S** represents a statically configured DNS server, and **D** represents a DNS server obtained dynamically through DHCP.
IP Address	IPv4 address of the DNS server.

display ip host

Syntax

display ip host [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip host** to display the host names and corresponding IPv4 addresses in the static domain name resolution table.

Examples

# Display the host names and corresponding IPv4 addresses in the static domain name resolution table.

```
<Sysname> display ip host
Host          Age      Flags        Address
My            0        static       1.1.1.1
Aa            0        static       2.2.2.4
```

Table 22 Command output

Field	Description
Host	Host name.
Age	Time to live. **0** means that the static mapping will never age out. You can only manually remove the static mappings between host names and IPv4 addresses.

Field	Description
Flags	Mapping type. Static represents static IPv4 domain name resolution.
Address	Host IPv4 address.

dns domain

Syntax

dns domain *domain-name*

undo dns domain [*domain-name*]

View

System view

Default level

2: System level

Parameters

domain-name: Domain name suffix, consisting of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. A domain name suffix may include case-insensitive letters, digits, hyphens (-), underscores (_), and dots (.), with a total length of 238 characters.

Description

Use **dns domain** to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use **undo dns domain** to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default. Only the provided domain name is resolved.

The domain name suffix configured with the **dns domain** command is applicable to both IPv4 DNS and IPv6 DNS.

You can configure a maximum of 10 domain name suffixes.

Related commands: **display dns domain**.

Examples

# Configure com as a DNS suffix.

```
<Sysname> system-view
[Sysname] dns domain com
```

dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

View

System view

Default level

2: System level

Parameters

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

Description

Use **dns dscp** to set the DSCP value for DNS packets.

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

By default, the DSCP value in DNS packets is 0.

Examples

# Set the DSCP value to 30 for DNS packets.

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

dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to disable DNS proxy.

By default, DNS proxy is disabled.

Examples

# Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns resolve

Syntax

dns resolve

undo dns resolve

View

System view

Default level

2: System level

Parameters

None

Description

Use **dns resolve** to enable dynamic domain name resolution.

Use **undo dns resolve** to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

This command is applicable to both IPv4 DNS and IPv6 DNS.

Examples

# Enable dynamic domain name resolution.

```
<Sysname> system-view
[Sysname] dns resolve
```

dns server

Syntax

In system view:

dns server *ip-address*

undo dns server [*ip-address*]

In interface view:

dns server *ip-address*

undo dns server *ip-address*

View

System view, interface view

Default level

2: System level

Parameters

ip-address: Specifies the IPv4 address of the DNS server.

Description

Use **dns server** to specify a DNS server.

Use **undo dns server** to remove DNS servers.

No DNS server is specified by default.

- You can configure up to six DNS servers, including those with IPv6 addresses, in system view, and up to six DNS servers on all interfaces of a device.
- A DNS server configured in system view has a higher priority than one configured in interface view. A DNS server configured earlier has a higher priority than one configured later in the same view.

A DNS server manually configured has a higher priority than one dynamically obtained through DHCP.

- Running the **undo dns server** command in system view will delete all DNS servers configured in system view and interface view. Running the **undo dns server** *ip-address* command in system view or interface view will delete the specific DNS server in system view or interface view.

Related commands: **display dns server**.

Examples

# Specify the DNS server 172.16.1.1 in system view.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

dns source-interface

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface

View

System view

Default level

2: System level

Parameters

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

Description

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

By default, no source interface for DNS packets is specified. The device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request.

The device uses the primary IP address of the specified source interface as the source IP address of a DNS request, which however is still forwarded through the output interface of the matching route.

Examples

# Specify VLAN-interface 2 as the source interface of DNS requests.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface2
```

dns spoofing

Syntax

dns spoofing *ip-address*

undo dns spoofing

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address used to spoof name query requests.

Description

Use **dns spoofing** to enable DNS spoofing.

Use **undo dns spoofing** to disable DNS spoofing.

By default, DNS spoofing is disabled.

With DNS proxy enabled but no DNS server specified or no DNS server reachable, a device cannot forward a DNS request, or answer the request. In this case, you can enable DNS spoofing on the device to spoof a reply with the configured IP address. Once a DNS server is reachable, the device will send DNS requests to the server and return replies to the requesting DNS clients.

If you repeatedly execute the **dns spoofing** command with different IP addresses specified, the latest configuration will overwrite the previous one.

Examples

# Enable DNS spoofing and specify the IP address as 1.1.1.1

```
<Sysname> system-view
[Sysname] dns spoofing 1.1.1.1
```

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Default level

2: System level

Parameters

hostname: Specifies the host name, consisting of 1 to 255 characters, including case-insensitive letters, numbers, hyphens (-), underscores (_), or dots (.). The host name must include at least one letter.

ip-address: Specifies the IPv4 address of the specified host in dotted decimal notation.

Description

Use **ip host** to create a host name to IPv4 address mapping in the static resolution table.

Use **undo ip host** to remove a mapping.

No mappings are created by default.

Each host name can correspond to only one IPv4 address. The IPv4 address you last assign to the host name will overwrite the previous one if there is any.

Related commands: **display ip host**.

Examples

# Map the IP address 10.110.0.1 to the host name aaa.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

reset dns host

Syntax

reset dns host [**ip** | **ipv6** | **naptr** | **srv**]

View

User view

Default level

2: System level

Parameters

ip: Clears the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Clears the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Clears the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Clears the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site.

Description

Use **reset dns host** to clear information of the dynamic DNS cache.

Without any keyword specified, this command clears the dynamic DNS cache information of all query types.

Related commands: **display dns host**.

Examples

# Clear the dynamic DNS cache information of all query types.

```
<Sysname> reset dns host
```

IRDP configuration commands

ip irdp

Syntax

ip irdp

undo ip irdp

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ip irdp** to enable IRDP on an interface.

Use **undo ip irdp** to disable IRDP on an interface.

IRDP is disabled on an interface by default.

IRDP configuration takes effect only when IRDP is enabled.

Examples

# Enable IRDP on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp
```

ip irdp address

Syntax

ip irdp address *ip-address preference*

undo ip irdp address *ip-address*

View

Interface view

Default level

2: System level

Parameters

ip-address: Specifies the proxy-advertised IP address.

preference: Specifies the preference of the proxy-advertised IP address, in the range of -2147483648 to 2147483647.

Description

Use **ip irdp address** to configure an IP address to be proxy-advertised by the interface.

Use **undo ip irdp address** to remove the proxy-advertised IP address.

Examples

# Specify the IP address 192.168.0.8 and its preference for VLAN-interface 1 to proxy-advertise.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp address 192.168.0.8 1600
```

ip irdp lifetime

Syntax

ip irdp lifetime *lifetime-value*

undo ip irdp lifetime

View

Interface view

Default level

2: System level

Parameters

lifetime-value: Specifies the lifetime of IP addresses advertised on the interface, in the range of 4 to 9000 seconds.

Description

Use **ip irdp lifetime** to set the lifetime of IP addresses advertised on an interface.

Use **undo ip irdp lifetime** to restore the default.

By default, the lifetime is 1800 seconds.

The lifetime of IP addresses cannot be shorter than the maximum advertising interval on an interface. Otherwise, a configuration error prompt is displayed.

Related commands: **ip irdp maxadvinterval**.

Examples

# Set the lifetime of IP addresses advertised on VLAN-interface 1 to 2000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp lifetime 2000
```

ip irdp maxadvinterval

Syntax

ip irdp maxadvinterval *interval-value*

undo ip irdp maxadvinterval

View

Interface view

Default level

2: System level

Parameters

interval-value: Specifies the maximum advertising interval in seconds, in the range of 4 to 1800.

Description

Use **ip irdp maxadvinterval** to set the maximum interval for advertising RAs on an interface.

Use **undo ip irdp maxadvinterval** to restore the default.

By default, the maximum advertising interval is 600 seconds.

The maximum advertising interval must be larger than the minimum interval. If not, the minimum interval will be automatically adjusted to 75% of the maximum interval.

The maximum advertising interval cannot be longer than the lifetime of advertised IP addresses. Otherwise, the lifetime will be automatically adjusted to a value three times the maximum interval.

Related commands: **ip irdp lifetime** and **ip irdp minadvinterval**.

Examples

# Set the maximum advertising interval on VLAN-interface 1 to 500 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp maxadvinterval 500
```

ip irdp minadvinterval

Syntax

ip irdp minadvinterval *interval-value*

undo ip irdp minadvinterval

View

Interface view

Default level

2: System level

Parameters

interval-value: Specifies the minimum advertising interval in seconds, in the range of 3 to 1800.

Parameters

Use **ip irdp minadvinterval** to set the minimum interval for advertising RAs on an interface.

Use **undo ip irdp minadvinterval** to restore the default.

By default, the minimum interval is 450 seconds.

The minimum advertising interval must be shorter than the maximum advertising interval. Otherwise, errors occur.

Related commands: **ip irdp maxadvinterval**.

Examples

# Set the minimum advertising interval on VLAN-interface 1 to 400 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp minadvinterval 400
```

ip irdp multicast

Syntax

ip irdp multicast

undo ip irdp multicast

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ip irdp multicast** to specify the multicast address 224.0.0.1 as the destination IP address of RAs sent on an interface.

Use **undo ip irdp multicast** to restore the default.

By default, the destination IP address is 255.255.255.255.

Examples

# Specify the multicast address 224.0.0.1 as the destination IP address for VLAN-interface 1 to send RAs.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp multicast
```

ip irdp preference

Syntax

ip irdp preference *preference-value*

undo ip irdp preference

View

Interface view

Default level

2: System level

Parameters

preference-value: Specifies the preference of IP addresses advertised on an interface, in the range of -2147483648 to 2147483647. The bigger the value, the higher the preference.

Description

Use **ip irdp preference** to configure the preference of IP addresses advertised on the interface.

Use **undo ip irdp preference** to restore the default.

By default, the preference of advertised IP addresses is 0.

Examples

# Configure preference 1 for IP addresses advertised on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp preference 1
```

IP performance optimization configuration commands

display fib

Syntax

display fib [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

acl *acl-number*: Displays FIB entries matching a specified ACL numbered from 2000 to 2999. If the specified ACL does not exist, all FIB entries are displayed.

ip-prefix *ip-prefix-name*: Displays FIB entries matching a specified IP prefix list, a string of 1 to 19 characters. If the specified IP prefix list does not exist, all FIB entries are displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib** to display FIB entries. If no parameters are specified, all FIB entries will be displayed.

Examples

# Display all FIB entries.

```
<Sysname> display fib
Destination count: 4    FIB entry count: 4

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.0.0/16       10.2.1.1    U       Vlan1         Null       Invalid
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
127.0.0.0/8       127.0.0.1   U       InLoop0       Null       Invalid
```

```
127.0.0.1/32      127.0.0.1   UH      InLoop0       Null       Invalid
```

# Display FIB information matching ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Destination count: 2    FIB entry count: 2

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.0.0/16       10.2.1.1    U       Vlan1        Null       Invalid
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
```

# Display all entries that contain the string **127** and start from the first one.

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
127.0.0.0/8       127.0.0.1   U       InLoop0       Null       Invalid
127.0.0.1/32      127.0.0.1   UH      InLoop0       Null       Invalid
```

Table 23 Command output

Field	Description
Destination count	Total number of destination addresses
FIB entry count	Total number of FIB entries
Destination/Mask	Destination address/length of mask
Nexthop	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
OutInterface	Outbound interface
InnerLabel	Inner label
Token	Link-state packet (LSP) index number

display fib *ip-address*

Syntax

display fib *ip-address* [*mask* | *mask-length*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Destination IP address, in dotted decimal notation.

mask: IP address mask.

mask-length: Length of IP address mask.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib** *ip-address* to display FIB entries that match the specified destination IP address.

If no mask or mask length is specified, the FIB entry that matches the destination IP address and has the longest mask will be displayed; if the mask is specified, the FIB entry that exactly matches the specified destination IP address will be displayed.

Examples

# Display the FIB entries that match the destination IP address of 10.2.1.1.

```
<Sysname> display fib 10.2.1.1
Destination count: 1    FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag     OutInterface  InnerLabel Token
10.2.1.1/32       127.0.0.1   UH       InLoop0       Null       Invalid
```

For description about the output, see Table 23.

display icmp statistics

Syntax

display icmp statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** **|** **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the ICMP statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display icmp statistics** to display ICMP statistics.

Related commands: **display ip interface** and **reset ip statistics**.

Examples

# Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats    0                  bad checksum           0
         echo           5                  destination unreachable 0
         source quench 0                  redirects              0
         echo reply     10                 parameter problem      0
         timestamp      0                  information request    0
         mask requests 0                  mask replies           0
         time exceeded 0
  Output:echo           10                 destination unreachable 0
         source quench 0                  redirects              0
         echo reply     5                  parameter problem      0
         timestamp      0                  information reply      0
         mask requests 0                  mask replies           0
         time exceeded 0
```

Table 24 Command output

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets
source quench	Number of input/output source quench packets

Field	Description
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output reply packets
time exceeded	Number of input/output expiration packets

display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id socket-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

socktype *sock-type*: Displays the socket information of this type. The sock type is in the range of 1 to 3, corresponding to TCP, UDP, and raw IP.

task-id: Displays the socket information of this task. Task ID is in the range of 1 to 255.

socket-id: Displays the information of the socket. Socket ID is in the range of 0 to 3072.

slot *slot-number*: Displays the socket information on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip socket** to display socket information.

Examples

# Display the TCP socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYD(38), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = HTTP(36), socketid = 1, Proto = 6,
LA = 0.0.0.0:80, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO

Task = ROUT(69), socketid = 10, Proto = 6,
LA = 0.0.0.0:179, FA = 192.168.1.45:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_REUSEPORT,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 4, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.52:1917,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 237, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 3, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.84:1503,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 11, Proto = 6,
LA = 192.168.1.40:1025, FA = 192.168.1.45:179,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR SO_LINGER,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = NTPT(37), socketid = 1, Proto = 17,
LA = 0.0.0.0:123, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = AGNT(51), socketid = 1, Proto = 17,
LA = 0.0.0.0:161, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RDSO(56), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = TRAP(52), socketid = 1, Proto = 17,
LA = 0.0.0.0:1025, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 0, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = RDSO(56), socketid = 2, Proto = 17,
LA = 0.0.0.0:1812, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = ROUT(69), socketid = 1, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RSVP(73), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
```

Table 25 Command output

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task number
socketid	Socket ID
Proto	Protocol number of the socket, indicating the protocol type that IP carries
LA	Local address and local port number
FA	Remote address and remote port number

Field	Description
sndbuf	Sending buffer size of the socket, in bytes
rcvbuf	Receiving buffer size of the socket, in bytes
sb_cc	Current data size in the sending buffer (available only for a TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

display ip statistics

Syntax

display ip statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the IP packet statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip statistics** to display statistics of IP packets.

Related commands: **display ip interface** and **reset ip statistics**.

Examples

# Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:   sum            7120            local            112
           bad protocol   0               bad format       0
           bad checksum   0               bad options      0
  Output:  forwarding     0               local            27
           dropped        0               no route         2
           compress fails 0
```

```
Fragment:input          0                output          0
         dropped        0
         fragmented     0                couldn't fragment 0
Reassembling:sum        0                timeouts        0
```

Table 26 Command output

Field		Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to be compressed
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that failed to be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

display tcp statistics

Syntax

display tcp statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp statistics** to display statistics of TCP traffic.

Related commands: **display tcp status** and **reset tcp statistics**.

Examples

# Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
     Total: 8457
     packets in sequence: 3660 (5272 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 1 (8 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 17 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 4625 (141989 bytes)
     duplicate ACK packets: 1702, too much ACK packets: 0

Sent packets:
     Total: 6726
     urgent packets: 0
     control packets: 21 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 6484 (141984 bytes) data packets retransmitted: 0 (0 bytes)
     ACK-only packets: 221 (177 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 1682, keepalive probe: 1682, Keepalive timeout, so connections
disconnected : 0
Initiated connections: 0, accepted connections: 22, established connections: 22
Closed connections: 49 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 27 Command output

Field		Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received

Field		Description
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout		Number of retransmission timer timeouts
connections dropped in retransmitted timeout		Number of connections broken due to retransmission timeouts
Keepalive timeout		Number of keepalive timer timeouts
keepalive probe		Number of keepalive probe packets sent
Keepalive timeout, so connections disconnected		Number of connections broken due to timeout of the keepalive timer
Initiated connections		Number of connections initiated
accepted connections		Number of connections accepted
established connections		Number of connections established
Closed connections		Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)
Packets dropped with MD5 authentication		Number of packets dropped by MD5 authentication
Packets permitted with MD5 authentication		Number of packets permitted by MD5 authentication

display udp statistics

Syntax

display udp statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp statistics** to display statistics of UDP packets.

Related commands: **reset udp statistics**.

Examples

# Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

Table 28 Command output

Field		Description
Received packets:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port

Field		Description
	not delivered, input socket full	Number of packets not delivered to an upper layer due to a full socket cache
	input packets missing pcb cache	Number of packets without matching protocol control block (PCB) cache
Sent packets:	Total	Total number of UDP packets sent

ip forward-broadcast (interface view)

Syntax

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

View

Interface view

Default level

2: System level

Parameters

acl *acl-number*: Specifies the ACL number, in the range of 2000 to 3999. Numbers between 2000 and 2999 are for basic ACLs, and between 3000 and 3999 are for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description

Use **ip forward-broadcast** to enable the interface to forward directed broadcasts to a directly connected network.

Use **undo ip forward-broadcast** to disable the interface from forwarding directed broadcasts to a directly connected network.

By default, an interface is disabled from forwarding directed broadcasts to a directly connected network.

Examples

# Enable VLAN-interface 2 to forward the directed broadcasts to a directly-connected network matching ACL 2001.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

ip forward-broadcast (system view)

Syntax

ip forward-broadcast

undo ip forward-broadcast

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip forward-broadcast** to enable the switch to receive directed broadcasts.

Use **undo ip forward-broadcast** to disable the switch from receiving directed broadcasts.

By default, the switch is disabled from receiving directed broadcast.

Examples

# Enable the switch to receive directed broadcasts.

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

ip redirects enable

Syntax

ip redirects enable

undo ip redirects

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip redirects enable** to enable sending of ICMP redirection packets.

Use **undo ip redirects** to disable sending of ICMP redirection packets.

This feature is disabled by default.

Examples

# Enable sending of ICMP redirect packets.

```
<Sysname> system-view
[Sysname] ip redirects enable
```

ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip ttl-expires enable** to enable sending of ICMP timeout packets.

Use **undo ip ttl-expires** to disable sending of ICMP timeout packets.

Sending ICMP timeout packets is disabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Examples

# Enable sending of ICMP timeout packets.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip unreachables enable** to enable sending of ICMP destination unreachable packets.

Use **undo ip unreachables** to disable sending of ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is disabled by default.

Examples

# Enable sending of ICMP destination unreachable packets.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

reset ip statistics

Syntax

reset ip statistics [**slot** *slot-number*]

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the IP packet statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset ip statistics** to clear statistics of IP packets.

Related commands: **display ip statistics** and **display ip interface**.

Examples

# Clear statistics of IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset tcp statistics** to clear statistics of TCP traffic.

Related commands: **display tcp statistics**.

Examples

# Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset udp statistics** to clear statistics of UDP traffic.

Examples

# Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

tcp path-mtu-discovery

Syntax

tcp path-mtu-discovery [**aging** *minutes* | **no-aging**]

undo tcp path-mtu-discovery

View

System view

Default level

2: System level

Parameters

aging *minutes*: Specifies the aging time of the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Do not age out the path MTU.

Description

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery, and disable all running path MTU timers. New TCP connections do not perform TCP path MTU discovery but existing TCP connections can still use TCP path MTU discovery.

By default, TCP path MTU discovery is disabled.

Examples

# Enable TCP path MTU discovery and set the path MTU age timer to 20 minutes.

```
<Sysname> system-view
[Sysname] tcp path-mtu-discovery aging 20
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

View

System view

Default level

2: System level

Parameters

time-value: Specifies the TCP finwait timer in seconds, in the range of 76 to 3,600.

Description

Use **tcp timer fin-timeout** to configure the length of the TCP finwait timer.

Use **undo tcp timer fin-timeout** to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

The actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer – 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout** and **tcp window**.

Examples

# Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

View

System view

Default level

2: System level

Parameters

time-value: Specifies the TCP synwait timer in seconds, in the range of 2 to 600.

Description

Use **tcp timer syn-timeout** to configure the length of the TCP synwait timer.

Use **undo tcp timer syn-timeout** to restore the default.

By default, the value of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout** and **tcp window**.

Examples

# Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Default level

2: System level

Parameters

window-size: Specifies the size of the send/receive buffer in KB, in the range of 1 to 32.

Description

Use **tcp window** to configure the size of the TCP send/receive buffer.

Use **undo tcp window** to restore the default.

The size of the TCP send/receive buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout** and **tcp timer syn-timeout**.

Examples

# Configure the size of the TCP send/receive buffer as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

UDP helper configuration commands

display udp-helper server

Syntax

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

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Displays information of forwarded UDP packets on a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp-helper server** to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

Examples

# Display the information of forwarded UDP packets on the interface VLAN-interface 1.

```
<Sysname> display udp-helper server interface vlan-interface 1
Interface name              Server address  Packets
Vlan-interface1              20.1.1.1         0
```

The output shows that the destination server corresponding to the interface VLAN-interface 1 is in the public network, the IP address of the destination server is 20.1.1.1, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax

reset udp-helper packet

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset udp-helper packet** to clear the statistics of forwarded UDP packets.

Related commands: **display udp-helper server**.

Examples

# Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **udp-helper enable** to enable UDP helper. A device enabled with UDP helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

Use **undo udp-helper enable** to disable UDP helper.

By default, UDP helper is disabled.

Examples

# Enable UDP helper

```
<Sysname> system-view
[Sysname] udp-helper enable
```

udp-helper port

Syntax

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

View

System view

Default level

2: System level

Parameters

port-number: Specifies the UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

dns: Forwards DNS data packets. The corresponding UDP port number is 53.

netbios-ds: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

netbios-ns: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

tacacs: Forwards terminal access controller access control system (TACACS) data packet. The corresponding UDP port number is 49.

tftp: Forwards TFTP data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description

Use **udp-helper port** to enable the forwarding of packets with the specified UDP port number.

Use **undo udp-helper port** to remove the configured UDP port numbers.

By default, no UDP port number is specified.

You can configure up to 256 UDP ports on a device.

All of the specified UDP port numbers will be removed if UDP helper is disabled.

Examples

# Forward broadcast packets with the UDP destination port number 100.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

Interface view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of the destination server, in dotted decimal notation.

Description

Use **udp-helper server** to specify the destination server to which UDP packets are forwarded.

Use **undo udp-helper server** to remove the destination server.

No destination server is configured by default.

You can configure up to 20 destination servers on an interface.

Without the *ip-address* argument, the **undo udp-helper server** command removes all the destination servers on an interface.

Related commands: **display udp-helper server**.

Examples

# Specify the IP address of the destination server in the public network as 192.1.1.2 on the VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

IPv6 basics configuration commands

display ipv6 fib

Syntax

display ipv6 fib [**acl6** *acl6-number* | **ipv6-prefix** *ipv6-prefix-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

acl6 *acl6-number*: Displays the IPv6 FIB entries permitted by a specified ACL. The ACL number is in the range of 2000 to 2999. If the specified ACL does not exist, all IPv6 FIB entries are displayed.

ipv6-prefix *ipv6-prefix-name*: Displays the IPv6 FIB entries matching a specified prefix list. The *ipv6-prefix-name* argument is a case-sensitive string of 1 to 19 characters. If the specified prefix list does not exist, all IPv6 FIB entries are displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib** to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

The device looks up a matching IPv6 FIB entry for forwarding an IPv6 packet.

Examples

# Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 1

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                                     PrefixLength : 128
NextHop     :    ::1                                      Flag           : HU
Label       :    NULL                                     Token          : 0
```

```
Interface  :    InLoopBack0
```

Table 29 Command output

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address
PrefixLength	Prefix length of the destination address
NextHop	Next hop
Flag	Route flag: • **U**—Usable route • **G**—Gateway route • **H**—Host route • **B**—Black hole route • **D**—Dynamic route • **S**—Static route
Label	Label
Token	LSP index number
Interface	Outgoing interface

display ipv6 fib *ipv6-address*

Syntax

display ipv6 fib *ipv6-address* [*prefix-length*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the Prefix length of the destination IPv6 address, in the range of 0 to 128.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib** *ipv6-address* to display the IPv6 FIB entry of the specified destination IPv6 address.

Without the *prefix-length* argument specified, this command displays the matching IPv6 FIB entry with the longest prefix.

With the *prefix-length* argument specified, this command displays the IPv6 FIB entry exactly matching the specified destination IPv6 address and prefix length.

Examples

# Display the matching IPv6 FIB entry with the longest prefix.

```
<Sysname> display ipv6 fib ::1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                                     PrefixLength : 128
NextHop    :    ::1                                      Flag           : HU
Label      :    NULL                                     Token          : 0
Interface  :    InLoopBack0
```

Table 30 Command output

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address
PrefixLength	Prefix length of the destination address
NextHop	Next hop
Flag	Route flag: • **U**—Usable route • **G**—Gateway route • **H**—Host route • **B**—Black hole route • **D**—Dynamic route • **S**—Static route
Label	Label
Token	LSP index number
Interface	Outgoing interface

display ipv6 interface

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Interface type.

interface-number: Interface number.

brief: Displays the brief IPv6 information of an interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 interface** to display the IPv6 information of an interface.

- If *interface-type interface-number* is not specified, the IPv6 information of all interfaces is displayed.
- If only *interface-type* is specified, the IPv6 information of the interfaces of the specified type is displayed.
- If *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed. If the **brief** keyword is also specified, the brief IPv6 information of the interface is displayed.

Examples

# Display the IPv6 information of 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
  Global unicast address(es):
    2001::1, subnet is 2001::/64
10::1234:56FF:FE65:4322, subnet is 10::/64 [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF65:4322
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                    0
  InTooShorts:                   0
  InTruncatedPkts:               0
  InHopLimitExceeds:             0
  InBadHeaders:                  0
  InBadOptions:                  0
  ReasmReqds:                    0
```

```
ReasmOKs:                0
InFragDrops:             0
InFragTimeouts:          0
OutFragFails:            0
InUnknownProtos:         0
InDelivers:              0
OutRequests:             0
OutForwDatagrams:        0
InNoRoutes:              0
InTooBigErrors:          0
OutFragOKs:              0
OutFragCreates:          0
InMcastPkts:             0
InMcastNotMembers:       0
OutMcastPkts:            0
InAddrErrors:            0
InDiscards:              0
OutDiscards:             0
```

Table 31 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: • **Administratively DOWN**—The VLAN interface is administratively down. The interface is shut down by using the **shutdown** command. • **DOWN**—The VLAN interface is administratively up but its physical state is down. No ports in the VLAN are up due to a connection or link failure. • **UP**—The administrative and physical states of the VLAN interface are both up.
Line protocol current state	Link layer protocol state of the interface: • **DOWN**—The link layer protocol state of the VLAN interface is down. • **UP**—The link layer protocol state of the VLAN interface is up.
IPv6 is enabled	IPv6 packet forwarding state of the interface (after an IPv6 address is configured for an interface, IPv6 is automatically enabled on it; IPv6 packet forwarding is enabled in the example).
link-local address	Link-local address configured for the interface.
Global unicast address(es)	Global unicast address(es) configured for the interface.
valid lifetime	Valid lifetime of the global unicast address obtained through stateless autoconfiguration.
preferred lifetime	Preferred lifetime of the global unicast address obtained through stateless autoconfiguration.
Joined group address(es)	Address(es) of multicast group(s) that the interface has joined.
MTU	Maximum transmission unit of the interface.

Field	Description
ND DAD is enabled, number of DAD attempts	Whether Duplicate Address Detection (DAD) is enabled. In this example, DAD is enabled. • If DAD is enabled, the number of attempts to send a Neighbor Solicitation (NS) message for DAD (configured by using the **ipv6 nd dad attempts** command) is also displayed. • If DAD is disabled, **ND DAD is disabled** is displayed. (You can disable DAD by setting the number of attempts to send an NS message for DAD to 0.)
ND reachable time	Time that a neighboring node is considered reachable after reachability has been confirmed.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses.
InReceives	All IPv6 packets received by the interface, including all types of error packets.
InTooShorts	Received IPv6 packets that are too short, with a length less than 40 bytes, for example.
InTruncatedPkts	Received IPv6 packets with a length less than that specified in the packets.
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the limit.
InBadHeaders	Received IPv6 packets with bad basic headers.
InBadOptions	Received IPv6 packets with bad extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of packets after reassembly rather than the number of fragments.
InFragDrops	IPv6 fragments discarded due to certain error.
InFragTimeouts	IPv6 fragments discarded because the interval for which they had stayed in the system buffer exceeded the specified period.
OutFragFails	Packets failed in fragmentation on the outbound interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that were delivered to application layer protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 application protocols.
OutForwDatagrams	Packets forwarded by the outbound interface.
InNoRoutes	IPv6 packets that were discarded because no matched route can be found.
InTooBigErrors	IPv6 packets that were discarded because they exceeded the path MTU.
OutFragOKs	Packets that were fragmented on the outbound interface.
OutFragCreates	Number of packet fragments after fragmentation on the outbound interface.
InMcastPkts	IPv6 multicast packets received on the interface.

Field	Description
InMcastNotMembers	Incoming IPv6 multicast packets that were discarded because the interface did not belong to the corresponding multicast groups.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	IPv6 packets that were discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that were discarded due to resource problems rather than packet content errors.
OutDiscards	Sent packets that were discarded due to resource problems rather than packet content errors.

# Display the brief IPv6 information of all interfaces.

```
<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          down        Unassigned
```

Table 32 Command output

Field	Description
*down: administratively down	The interface is down. The interface is 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 does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface.
Physical	Physical state of the interface: • ***down**—The VLAN interface is administratively down. The interface is shut down using the **shutdown** command. • **down**—The VLAN interface is administratively up but its physical state is down. No port in the VLAN is up due to a connection or link failure. • **up**—The administrative and physical states of the VLAN interface are both up.
Protocol	Link layer protocol state of the interface: • **down**—The network layer protocol state of the VLAN interface is down. • **up**—The network layer protocol state of the VLAN interface is up.
IPv6 Address	IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. If no address is configured for the interface, **Unassigned** will be displayed.

display ipv6 nd snooping

Syntax

display ipv6 nd snooping [*ipv6-address* | **vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies an IPv6 address.

vlan *vlan-id*: Displays ND snooping entries in the specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd snooping** to display ND snooping entries.

If no parameter is specified, this command displays all ND snooping entries.

Examples

# Display the ND snooping entries of VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1
IPv6 Address                  MAC Address     VID  Interface      Aging Status
4001::1                       0015-e944-a947  1    GE1/0/1         25    Bound
 ---- Total entries on VLAN 1: 1 ----
```

Table 33 Command output

Field	Description
IPv6 Address	IPv6 address of an ND snooping entry.
MAC Address	MAC address of an ND snooping entry.
VID	VLAN ID.
Interface	Receiving port of an ND snooping entry.
Aging	Aging time of an ND snooping entry, in minutes.
Status	ND snooping entry status, which can be Bound or Probe.
Total entries on VLAN 1	Total number of ND snooping entries of VLAN 1.

display ipv6 neighbors

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies the IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

slot *slot-number*: Displays the neighbor information on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 neighbors** to display neighbor information.

You can use the **reset ipv6 neighbors** command to clear specific IPv6 neighbor information.

Related commands: **ipv6 neighbor**, **reset ipv6 neighbors**.

Examples

# Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
                Type: S-Static    D-Dynamic
IPv6 Address             Link-layer       VID  Interface State   T   Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800  N/A  GE1/0/1    REACH   S    -
```

Table 34 Command output

Field	Description
IPv6 Address	IPv6 address of a neighbor.
Link-layer	Link layer address (MAC address) of a neighbor.
VID	VLAN to which the interface connected with a neighbor belongs.
Interface	Interface connected with a neighbor.
State	State of a neighbor: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—The reachability of the neighbor is unknown. The device sends an NS message after a delay. • **PROBE**—The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Type of neighbor information, including static configuration (represented by **S**) and dynamic acquisition (represented by **D**).
Age	For a static entry, a hyphen (-) is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, a pound sign (#) is displayed (for a neighbor acquired dynamically).

display ipv6 neighbors count

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

dynamic: Displays the total number of all neighbor entries acquired dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Displays the total number of neighbor entries on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

interface *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

vlan *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 neighbors count** to display the total number of neighbor entries satisfying the specified condition.

Examples

# Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  2
```

display ipv6 pathmtu

Syntax

display ipv6 pathmtu { *ipv6-address* | **all** | **dynamic** | **static** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address for which the path MTU information is to be displayed.

all: Displays all path MTU information on the public network.

dynamic: Displays all dynamic path MTU information.

static: Displays all static path MTU information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 pathmtu** to display the IPv6 path MTU information.

Examples

# Display all path MTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address ZoneID   PathMTU     Age      Type
 fe80::12                0        1300        40       Dynamic
 2222::3                 0        1280        --       Static
```

Table 35 Command output

Field	Description
IPv6 Destination Address	Destination IPv6 address.
ZoneID	ID of address zone, currently invalid.
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, two consecutive hyphens (--) are displayed.
Type	The path MTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax

display ipv6 socket [**socktype** *socket-type*] [*task-id socket-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

socktype *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. The value 1 represents a TCP socket, value 2 a UDP socket, and value 3 a raw socket.

task-id: Displays the socket information of the task. The task ID is in the range of 1 to 255.

socket-id: Displays the information of the socket. The socket ID is in the range of 0 to 3072.

slot *slot-number*: Displays the socket information on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 socket** to display socket information.

With no parameter specified, this command displays the information about all the sockets; with only the socket type specified, the command displays the information about sockets of the specified type; with the socket type, task ID and socket ID specified, the command displays the information about the specified socket.

Examples

# Display the information of all sockets.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = AGNT(51), socketid = 2, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = TRAP(52), socketid = 2, Proto = 17,
LA = ::->1024, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option =,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(86), socketid = 5, Proto = 89,
LA = ::, FA = ::,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR,
socket state = SS_PRIV SS_ASYNC
```

Table 36 Command output

Field	Description
SOCK_STREAM	TCP socket.

Field	Description
SOCK_DGRAM	UDP socket.
SOCK_RAW	Raw IP socket.
Task	Task name and ID of the created socket.
socketid	ID assigned by the kernel to the created socket.
Proto	Protocol type, for example, **6** indicates TCP and **17** indicates UDP.
LA	Local address and local port number.
FA	Remote address and remote port number.
sndbuf	Size of the send buffer.
rcvbuf	Size of the receive buffer.
sb_cc	Number of bytes sent by the send buffer.
rb_cc	Number of bytes received by the receive buffer.
socket option	Socket option set by the application: • **SO_ACCEPTCONN**—Detects connection request at the server end. • **SO_REUSEADDR**—Allows for reuse of a local address. • **SO_REUSEPORT**—Allows for reuse of a local port.
socket state	State of the socket.

display ipv6 statistics

Syntax

display ipv6 statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the IPv6 and ICMPv6 packets statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 statistics** to display statistics of IPv6 packets and ICMPv6 packets.

You can use the **reset ipv6 statistics** command to clear all IPv6 and ICMPv6 packet statistics.

Examples

# Display the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> display ipv6 statistics
  IPv6 Protocol:

    Sent packets:
      Total:      0
        Local sent out:      0            forwarded:          0
        raw packets:         0            discarded:          0
        routing failed:      0            fragments:          0
        fragments failed:    0

    Received packets:
      Total:      0
        local host:          0            hopcount exceeded:  0
        format error:        0            option error:       0
        protocol error:      0            fragments:          0
        reassembled:         0            reassembly failed:  0
        reassembly timeout:  0

  ICMPv6 protocol:

    Sent packets:
      Total:      0
        unreached:           0               too big:              0
        hopcount exceeded:   0               reassembly timeout:   0
        parameter problem:   0

        echo request:        0               echo replied:         0
        neighbor solicit:    0               neighbor advert:      0
        router solicit:      0               router advert:        0
        redirected:          0               router renumbering:   0
      Send failed:
        ratelimited:     0               other errors:     0

    Received packets:
      Total:      0
        checksum error:      0              too short:             0
        bad code:            0

        unreached:           0              too big:               0
        hopcount exceeded:   0              reassembly timeout:    0
        parameter problem:   0              unknown error type:    0
        echo request:        0              echo replied:          0
        neighbor solicit:    0              neighbor advert:       0
        router solicit:      0              router advert:         0
        redirected:          0              router renumbering:    0
        unknown info type:   0
      Deliver failed:
        bad length:          0               ratelimited:          0
```

Table 37 Command output

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets: • Total number of packets sent and forwarded locally • Number of packets sent locally • Number of forwarded packets • Number of packets sent via raw socket • Number of discarded packets • Number of packets failing to be routed • Number of sent fragment packets • Number of fragments failing to be sent
Received packets: Total: 0 local host: 0 hopcount exceeded: 0 format error: 0 option error: 0 protocol error:0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets: • Total number of received packets • Number of packets received locally • Number of packets exceeding the hop limit • Number of packets in an incorrect format • Number of packets with incorrect options • Number of packets with incorrect protocol • Number of received fragment packets • Number of reassembled packets • Number of packets failing to be reassembled • Number of packets whose reassembly times out
ICMPv6 protocol:	Statistics of ICMPv6 packets

Field	Description
Sent packets: Total: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of sent ICMPv6 packets: • Total number of sent packets • Number of Destination Unreachable packets • Number of Packet Too Big packets • Number of Hop Limit Exceeded packets • Number of Fragment Reassembly Time Exceeded packets • Number of Parameter Problem packets • Number of Echo Request packets • Number of Echo Reply packets • Number of neighbor solicitation packets • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of Redirect packets • Number of router renumber (RR) packets • Number of packets failing to be sent due to rate limitation • Number of packets with other errors
Received packets: Total: 0 checksum error: 0 too short: 0 bad code: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets: • Total number of received packets • Number of packets with checksum errors • Number of too small packets • Number of packets with error codes • Number of Destination Unreachable packets • Number of Packet Too Big packets • Number of Hop Limit Exceeded packets • Number of Fragment Reassembly Times Exceeded packets • Number of Parameter Problem packets • Number of packets with unknown errors • Number of Echo Request packets • Number of Echo Reply packets • Number of neighbor solicitation messages • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of Redirect packets • Number of RR packets • Number of unknown type of packets • Number of packets with a incorrect size • Number of packets failing to be received due to rate limitation

display tcp ipv6 statistics

Syntax

display tcp ipv6 statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp ipv6 statistics** to display IPv6 TCP connection statistics.

You can use the **reset tcp ipv6 statistics** command to clear statistics of all IPv6 TCP packets.

Examples

# Display the statistics of IPv6 TCP connections.

```
<Sysname> display tcp ipv6 statistics
Received packets:
     Total: 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets with data after window: 0 (0 bytes)
     packets after close: 0

     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
     Total: 0
     urgent packets: 0
     control packets: 0 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
     ACK only packets: 0 (0 delayed)
```

```
Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections disconnected :
0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 38 Command output

Field	Description
Received packets: Total: 0 packets in sequence: 0 (0 bytes) window probe packets: 0 window update packets: 0 checksum error: 0 offset error: 0 short error: 0 duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes) out-of-order packets: 0 (0 bytes) packets with data after window: 0 (0 bytes) packets after close: 0 ACK packets: 0 (0 bytes) duplicate ACK packets: 0 too much ACK packets: 0	Statistics of received packets: • Total number of received packets • Number of packets received in sequence • Number of window probe packets • Number of window size update packets • Number of packets with checksum errors • Number of packets with offset errors • Number of packets whose total length is less than specified by the packet header • Number of duplicate packets • Number of partially duplicate packets • Number of out-of-order packets • Number of packets exceeding the size of the receiving window • Number of packets received after the connection is closed • Number of ACK packets • Number of duplicate ACK packets • Number of excessive ACK packets
Sent packets: Total: 0 urgent packets: 0 control packets: 0 (including 0 RST) window probe packets: 0 window update packets: 0 data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes) ACK only packets: 0 (0 delayed)	Statistics of sent packets: • Total number of packets • Number of packets containing an urgent indicator • Number of control packets • Number of window probe packets • Number of window update packets • Number of data packets • Number of retransmitted packets • Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts

Field	Description
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)
Packets dropped with MD5 authentication	Number of packets that fail the MD5 authentication and are dropped
Packets permitted with MD5 authentication	Number of packets that pass the MD5 authentication

display tcp ipv6 status

Syntax

display tcp ipv6 status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp ipv6 status** to display the IPv6 TCP connection status, including the IPv6 TCP control block address, local and peer IPv6 addresses, and status of the IPv6 TCP connection.

Examples

# Display the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
*: TCP6 MD5 Connection
TCP6CB        Local Address       Foreign Address      State
045d8074      ::->21                ::->0              Listening
```

Table 39 Command output

Field	Description
*: TCP6 MD5 Connection	The asterisk (*) indicates that the TCP6 connection is secured with MD5 authentication.
TCP6CB	IPv6 TCP control block address (hexadecimal).
Local Address	Local IPv6 address.
Foreign Address	Remote IPv6 address.
State	IPv6 TCP connection status: • Closed • Listening • Syn_Sent • Syn_Rcvd • Established • Close_Wait • Fin_Wait1 • Closing • Last_Ack • Fin_Wait2 • Time_Wait

display udp ipv6 statistics

Syntax

display udp ipv6 statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp ipv6 statistics** to display the statistics of IPv6 UDP packets.

You can use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

Examples

# Display the statistics of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

Table 40 Command output

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error
shorter than header	Total number of IPv6 UDP packets whose total length is less than that specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of received unicast packets without any socket
broadcast/multicast(no socket on port)	Total number of received broadcast/multicast packets without any socket
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the protocol control block (PCB) cache

ipv6

Syntax

ipv6

undo ipv6

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6** to enable IPv6.

Use **undo ipv6** to disable IPv6.

By default, IPv6 is disabled.

Examples

# Enable IPv6.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*]

View

Interface view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 1 to 128.

Description

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to remove the IPv6 address from the interface.

By default, no global unicast address is configured for an interface.

Except for the link-local address automatically obtained and the link-local address generated through stateless autoconfiguration, all IPv6 addresses will be removed from the interface if the **undo ipv6 address** command is executed without any parameter specified.

Examples

# Set the global IPv6 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

Syntax

ipv6 address *ipv6-address/prefix-length* **anycast**

undo ipv6 address *ipv6-address/prefix-length* **anycast**

View

Interface view

Default level

2: System level

Parameters

ipv6-address/prefix-length: Specifies an IPv6 anycast address and its prefix length. The prefix length ranges 1 to 128.

Description

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to remove the IPv6 anycast address from the interface.

By default, no IPv6 anycast address is configured for an interface.

Examples

# Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

ipv6 address auto

Syntax

ipv6 address auto

undo ipv6 address auto

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 address auto** to enable the stateless address autoconfiguration function on the interface. With this function enabled, the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this function.

The stateless address autoconfiguration function is disabled by default.

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically, which can be removed only by executing the **undo ipv6 address auto** command.

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

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to remove the automatically generated link-local address for the interface.

By default, no link-local address is configured on an interface, and a link-local address will be automatically generated after a global IPv6 unicast address is configured for the interface.

- After an IPv6 global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The **undo ipv6 address auto link-local** command can only remove the link-local addresses generated through the **ipv6 address auto link-local** command. After the **undo ipv6 address auto link-local** command is used on an interface that has an IPv6 global unicast address configured, the interface still has a link-local address. If the interface has no IPv6 global unicast address configured, it will have no link-local address.
- Manual assignment takes precedence over automatic generation. If you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated address. If you first use manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned address. If you delete the manually assigned address, the automatically generated link-local address is validated. For more information about manual assignment of an IPv6 link-local address, see the **ipv6 address link-local** command.

Examples

# Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

ipv6 address eui-64

Syntax

ipv6 address *ipv6-address***/***prefix-length* **eui-64**

undo ipv6 address *ipv6-address/prefix-length* **eui-64**

View

Interface view

Default level

2: System level

Parameters

ipv6-address/prefix-length: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an EUI-64 IPv6 address.

Description

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to remove the configured EUI-64 IPv6 address for the interface.

By default, no EUI-64 IPv6 address is configured for an interface.

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface identifier and is displayed by using 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 length of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View

Interface view

Default level

2: System level

Parameters

ipv6-address: IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Description

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to remove the configured link-local address for the interface.

Manual assignment takes precedence over automatic generation. If you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For automatic generation of an IPv6 link-local address, 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
```

ipv6 hoplimit-expires enable

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 hoplimit-expires enable** to enable the sending of ICMPv6 Time Exceeded packets.

Use **undo ipv6 hoplimit-expires** to disable the sending of ICMPv6 Time Exceeded packets.

By default, the sending of ICMPv6 Time Exceeded packets is enabled.

After you disable the sending of ICMPv6 Time Exceeded packets, the device will still send Fragment Reassembly Time Exceeded packets.

Examples

# Disable the sending of ICMPv6 Time Exceeded packets.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires
```

ipv6 icmp-error

Syntax

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

View

System view

Default level

2: System level

Parameters

bucket *bucket-size*: Number of tokens in the token bucket, in the range of 1 to 200.

ratelimit *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period "0" indicates that the number of ICMPv6 error packets sent is not restricted.

Description

Use **ipv6 icmp-error** to configure the size and update period of the token bucket.

Use **undo ipv6 icmp-error** to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. A maximum of 10 ICMPv6 error packets can be sent within 100 milliseconds.

Examples

# Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 icmpv6 multicast-echo-reply enable

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to disable replying to multicast echo requests.

By default, the device is disabled from replying to multicast echo requests.

Examples

# Enable replying to multicast echo requests.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 nd autoconfig managed-address-flag

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

By default, the M flag is set to **0** so that the host can acquire an IPv6 address through stateless autoconfiguration.

Examples

# Configure the host to acquire an IPv6 address through stateful autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 so that the host can acquire information other than IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

By default, the O flag is set to **0** so that the host can acquire other information through stateless autoconfiguration.

Examples

# Configure the host to acquire information other than IPv6 address through stateless autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

View

Interface view

Default level

2: System level

Parameters

value: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. The default value is 1. When it is set to 0, DAD is disabled.

Description

Use **ipv6 nd dad attempts** to configure the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

By default, the number of attempts to send an NS message for DAD is 1.

Related commands: **display ipv6 interface**.

Examples

# Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax

ipv6 nd hop-limit *value*

undo ipv6 nd hop-limit

View

System view

Default level

2: System level

Parameters

value: Specifies the number of hops, in the range of 0 to 255. When it is set to 0, the Hop Limit field in RA messages sent by the device is 0. The number of hops is determined by the requesting device itself.

Description

Use **ipv6 nd hop-limit** to configure the hop limit advertised by the device.

Use **undo ipv6 nd hop-limit** to restore the default hop limit.

By default, the hop limit advertised by the device is 64.

Examples

# Set the hop limit advertised by the device to 100.

```
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

ipv6 nd ns retrans-timer

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

View

Interface view

Default level

2: System level

Parameters

value: Specifies the interval for retransmitting an NS message in milliseconds, in the range of 1000 to 4294967295.

Description

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message. The local interface retransmits an NS message at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

By default, the local interface sends NS messages at an interval of 1000 millisecond and the Retrans Timer field in the RA messages sent is 0, so that the interval for retransmitting an NS message is determined by the receiving device.

Related commands: **display ipv6 interface**.

Examples

# Specify VLAN-interface 100 to retransmit NS messages at intervals of 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

ipv6 nd nud reachable-time

Syntax

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

View

Interface view

Default level

2: System level

Parameters

value: Specifies the neighbor reachable time in milliseconds, in the range of 1 to 3600000.

Description

Use **ipv6 nd nud reachable-time** to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Time field in RA messages sent by the local interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

By 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, so that the reachable time is determined by the receiving device.

Related commands: **display ipv6 interface**.

Examples

# Set the neighbor reachable time on VLAN-interface 100 to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

ipv6 nd ra halt

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd ra halt** to enable RA message suppression.

Use **undo ipv6 nd ra halt** to disable RA message suppression.

By default, RA messages are suppressed.

Examples

# Suppress RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra halt
```

ipv6 nd ra interval

Syntax

ipv6 nd ra interval *max-interval-value min-interval-value*

undo ipv6 nd ra interval

View

Interface view

Default level

2: System level

Parameters

max-interval-value: Specifies the maximum interval for advertising RA messages in seconds, in the range of 4 to 1800.

min-interval-value: Specifies the minimum interval for advertising RA messages in seconds, in the range of 3 to 1350.

Description

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use **undo ipv6 nd ra interval** to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

The minimum interval should be three-fourths of the maximum interval or less.

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

# Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

ipv6 nd ra no-advlinkmtu

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

View

Interface view

Default level

2: System level

Parameters

None

Description

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.

By default, RA messages contain the MTU option.

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

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix/prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix/prefix-length* }

View

Interface view

Default level

2: System level

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 seconds, in the range of 0 to 4294967295.

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4294967295.

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If this keyword is not provided, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

Description

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information with valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (seven days).

Examples

# Configure the prefix information for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

ipv6 nd ra router-lifetime

Syntax

ipv6 nd ra router-lifetime *value*

undo ipv6 nd ra router-lifetime

View

Interface view

Default level

2: System level

Parameters

value: Specifies the router lifetime in seconds, in the range of 0 to 9000. When it is set to 0, the device does not serve as the default router.

Description

Use **ipv6 nd ra router-lifetime** to configure the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

By default, the router lifetime in RA messages is 1800 seconds.

The router lifetime in RA messages should be greater than or equal to the advertising interval.

Examples

# Set the router lifetime in RA messages on VLAN-interface 100 to 1000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

ipv6 nd snooping enable

Syntax

ipv6 nd snooping enable

undo ipv6 nd snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd snooping enable** to enable ND snooping.

Use **undo ipv6 nd snooping enable** to restore the default.

By default, ND snooping is disabled.

Examples

# Enable ND snooping for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] ipv6 nd snooping enable
```

ipv6 nd snooping enable global

Syntax

ipv6 nd snooping enable global

undo ipv6 nd snooping enable global

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd snooping enable global** to enable ND snooping based on global unicast addresses (the devices use DAD NS messages containing global unicast addresses to create ND snooping entries).

Use **undo ipv6 nd snooping enable global** to restore the default.

By default, ND snooping based on global unicast addresses is disabled.

Examples

# Enable ND snooping based on global unicast addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable global
```

ipv6 nd snooping enable link-local

Syntax

ipv6 nd snooping enable link-local

undo ipv6 nd snooping enable link-local

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd snooping enable link-local** to enable ND snooping based on link local addresses (the devices use DAD NS messages containing link local addresses to create ND snooping entries).

Use **undo ipv6 nd snooping enable link-local** to restore the default.

By default, ND snooping based on link local addresses is disabled.

Examples

# Enable ND snooping based on link local addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable link-local
```

ipv6 nd snooping max-learning-num

Syntax

ipv6 nd snooping max-learning-num *number*

undo ipv6 nd snooping max-learning-num

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of ND snooping entries that can be learned by the interface, in the range of 0 to 4096.

Description

Use **ipv6 nd snooping max-learning-num** to configure the maximum number of ND snooping entries that can be learned on the interface.

Use **undo ipv6 nd snooping max-learning-num** to restore the default.

By default, the number of ND snooping entries that an interface can learn is not limited.

Examples

# Set the maximum number of ND snooping entries that can be learned on Layer 2 Ethernet port GigabitEthernet 1/0/1 to 1000.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 1000
```

# Set the maximum number of ND snooping entries that can be learned on Layer 2 aggregate interface 1 to 1000.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping max-learning-num 1000
```

ipv6 nd snooping uplink

Syntax

ipv6 nd snooping uplink

undo ipv6 nd snooping uplink

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd snooping uplink** to configure the interface as an uplink interface and disable it from learning ND snooping entries.

Use **undo ipv6 nd snooping uplink** to restore the default.

By default, when ND snooping is enabled on the device, an interface is allowed to learn ND snooping entries.

Examples

# Configure Layer 2 Ethernet port GigabitEthernet 1/0/1 as an uplink interface and disable it from learning ND snooping entries.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping uplink
```

# Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an uplink interface and disable it form learning ND snooping entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping uplink
```

ipv6 neighbor

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

undo ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

View

System view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address of the static neighbor entry (48 bits long, 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.

Description

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to remove a static neighbor entry.

You can use a Layer 3 VLAN interface or a Layer 2 port in the VLAN to configure a static neighbor entry.

- If the first method is used, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry will go into the REACH state.
- If the second method is used, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After the static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify the static neighbor entry uniquely and the entry will be in the REACH state.

To remove a static neighbor entry, you only need to specify the corresponding VLAN interface and the neighbor address.

Related commands: **display ipv6 neighbors**.

Examples

# Configure a static neighbor entry for Layer 2 port GigabitEthernet 1/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 GigabitEthernet 1/0/1
```

ipv6 neighbor stale-aging

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

View

System view

Default level

2: System level

Parameters

aging-time: Age timer for ND entries in stale state, ranging from 1 to 24 hours.

Description

Use **ipv6 neighbor stale-aging** to set the age timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

By default, the age timer for ND entries in stale state is four hours.

Examples

# Set the age timer for ND entries in stale state to two hours.

```
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 2
```

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

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

Default level

2: System level

Parameters

number: Maximum number of neighbors that can be dynamically learned by the interface, ranging from 1 to 512.

Description

Use **ipv6 neighbors max-learning-num** to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

By default, a Layer 2 interface does not limit the number of neighbors dynamically learned. A Layer 3 interface can learn up to 512 neighbors dynamically.

Examples

# Set the maximum number of neighbors that can be dynamically learned on VLAN-interface 100 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Syntax

ipv6 pathmtu *ipv6-address* [*value*]

undo ipv6 pathmtu *ipv6-address*

View

System view

Default level

2: System level

Parameters

ipv6-address: IPv6 address.

value: Path MTU of a specified IPv6 address, ranging from 1280 to 10000 bytes.

Description

Use **ipv6 pathmtu** to configure a static path MTU for a specified IPv6 address.

Use **undo ipv6 pathmtu** to remove the path MTU configuration for a specified IPv6 address.

By default, no static path MTU is configured.

Examples

# Configure a static path MTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

ipv6 pathmtu age

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

View

System view

Default level

2: System level

Parameters

age-time: Specifies the aging time for path MTU in minutes, in the range of 10 to 100.

Description

Use **ipv6 pathmtu age** to configure the aging time for a dynamic path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

By default, the aging time is 10 minutes.

The aging time is invalid for a static path MTU.

Related commands: **display ipv6 pathmtu**.

Examples

# Set the aging time for a dynamic path MTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

ipv6 prefer temporary-address

Syntax

ipv6 prefer temporary-address [*valid-lifetime preferred-lifetime*]

undo ipv6 prefer temporary-address

View

System view

Default level

2: System level

Parameters

valid-lifetime: Specifies the valid lifetime of temporary IPv6 addresses in seconds, in the range of 600 to 4294967295. The default valid lifetime is 604800 seconds, that is, seven days.

preferred-lifetime: Specifies the preferred lifetime of temporary IPv6 addresses in seconds, in the range of 600 to 4294967295. The default valid lifetime is 86400 seconds, that is, one day.

Description

Use **ipv6 prefer temporary-address** to configure the system to generate and preferably use the temporary IPv6 address of the sending interface as the source address of the packet to be sent.

Use **undo ipv6 prefer temporary-address** to disable the system from generating temporary IPv6 addresses and remove existing temporary IPv6 addresses.

By default, the system does not generate or use any temporary IPv6 address.

- Configure the valid lifetime greater than (or equal to) the preferred lifetime.
- Enable stateless address autoconfiguration before configuring this function.
- The preferred lifetime of a temporary IPv6 address takes the value of the preferred lifetime of the address prefix, or the value of the preferred lifetime you configure for temporary IPv6 addresses minus DESYNC_FACTOR (which is a random number ranging 0 to 600, in seconds), whichever is smaller.
- The valid lifetime of a temporary IPv6 address takes the value of the valid lifetime of the address prefix, or the value of the valid lifetime you configure for temporary IPv6 addresses, whichever is smaller.

Examples

# Configure the system to generate and preferably use the temporary IPv6 address of the sending interface as the source address of the packet to be sent.

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

ipv6 unreachables enable

Syntax

ipv6 unreachables enable

undo ipv6 unreachables

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 unreachables enable** to enable sending of ICMPv6 destination unreachable packets.

Use **undo ipv6 unreachables** to disable sending of ICMPv6 destination unreachable packets.

By default, sending of ICMPv6 destination unreachable packets is disabled.

Examples

# Enable sending of ICMPv6 destination unreachable packets.

```
<Sysname> system-view
[Sysname] ipv6 unreachables enable
```

local-proxy-nd enable

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

View

VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to restore the default.

By default, local ND proxy is disabled.

Examples

# Enable local ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] local-proxy-nd enable
```

proxy-nd enable

Syntax

proxy-nd enable

undo proxy-nd enable

View

VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **proxy-nd enable** to enable ND proxy.

Use **undo proxy-nd enable** to restore the default.

By default, ND proxy is disabled.

Examples

# Enable ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] proxy-nd enable
```

reset ipv6 nd snooping

Syntax

reset ipv6 nd snooping [*ipv6-address* | **vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

ipv6-address: Clears the ND snooping entries of the specified IPv6 address.

vlan *vlan-id*: Clears the ND snooping entries of the specified VLAN. The VLAN ID ranges 1 to 4094.

Description

Use **reset ipv6 nd snooping** to clear ND snooping entries.

If no parameter is specified, this command clears all ND snooping entries.

Examples

# Clear all ND snooping entries on VLAN 1.

```
<Sysname> reset ipv6 nd snooping vlan 1
```

reset ipv6 neighbors

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

View

User view

Default level

2: System level

Parameters

all: Clears static and dynamic neighbor information on all interfaces.

dynamic: Clears dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

slot *slot-number*: Clears the dynamic neighbor information on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

static: Clears static neighbor information on all interfaces.

Description

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

You can use the **display ipv6 neighbors** command to display the current IPv6 neighbor information.

Examples

# Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

# Clear dynamic neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

# Clear all neighbor information on GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 neighbors interface GigabitEthernet 1/0/1
```

reset ipv6 pathmtu

Syntax

reset ipv6 pathmtu { **all** | **static** | **dynamic** }

View

User view

Default level

2: System level

Parameters

all: Clears all path MTUs.

static: Clears all static path MTUs.

dynamic: Clears all dynamic path MTUs.

Description

Use **reset ipv6 pathmtu** to clear the path MTU information.

Examples

# Clear all path MTUs.

```
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax

reset ipv6 statistics [**slot** *slot-number*]

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the IPv6 and ICMPv6 packets statistics on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset ipv6 statistics** to clear the statistics of IPv6 packets and ICMPv6 packets.

You can use the **display ipv6 statistics** command to display the statistics of IPv6 and ICMPv6 packets.

Examples

# Clear the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax

reset tcp ipv6 statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset tcp ipv6 statistics** to clear the statistics of all IPv6 TCP connections.

You can use the **display tcp ipv6 statistics** command to display the statistics of IPv6 TCP connections.

Examples

# Clear the statistics of all IPv6 TCP connections.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax

reset udp ipv6 statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset udp ipv6 statistics** to clear the statistics of all IPv6 UDP packets.

You can use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

Examples

# Clear the statistics of all IPv6 UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax

tcp ipv6 timer fin-timeout *wait-time*

undo tcp ipv6 timer fin-timeout

View

System view

Default level

2: System level

Parameters

wait-time: Specifies the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3,600.

Description

Use **tcp ipv6 timer fin-timeout** to set the finwait timer for IPv6 TCP connections.

Use **undo tcp ipv6 timer fin-timeout** to restore the default.

By default, the length of the finwait timer is 675 seconds.

Examples

# Set the finwait timer length of IPv6 TCP connections to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer fin-timeout 800
```

tcp ipv6 timer syn-timeout

Syntax

tcp ipv6 timer syn-timeout *wait-time*

undo tcp ipv6 timer syn-timeout

View

System view

Default level

2: System level

Parameters

wait-time: Specifies the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.

Description

Use **tcp ipv6 timer syn-timeout** to set the synwait timer for IPv6 TCP connections

Use **undo tcp ipv6 timer syn-timeout** to restore the default.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

Examples

# Set the synwait timer length of IPv6 TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

tcp ipv6 window

Syntax

tcp ipv6 window *size*

undo tcp ipv6 window

View

System view

Default level

2: System level

Parameters

size: Specifies the size of the IPv6 TCP send/receive buffer in KB (kilobyte), in the range of 1 to 32.

Description

Use **tcp ipv6 window** to set the size of the IPv6 TCP send/receive buffer.

Use **undo tcp ipv6 window** to restore the default.

By default, the size of the IPv6 TCP send/receive buffer is 8 KB.

Examples

# Set the size of the IPv6 TCP send/receive buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

DHCPv6 configuration commands

DHCPv6 common configuration commands

display ipv6 dhcp duid

Syntax

display ipv6 dhcp duid [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp duid** to display the DUID of the local device.

Examples

# Display the DUID of the device.

```
<Sysname> display ipv6 dhcp duid
The DUID of this device: 0003-0001-00e0-fc00-5552
```

DHCPv6 server configuration commands

display ipv6 dhcp pool

Syntax

display ipv6 dhcp pool [*pool-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pool-number: Displays the details about the address pool specified by the pool number. If no pool number is specified, all address pool information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp pool** to display DHCPv6 address pool information.

Examples

# Display all address pool information.

```
<Sysname> display ipv6 dhcp pool
Pool                Prefix-pool
1                   1
2                   Not configured
```

Table 41 Command output

Field	Description
Pool	DHCPv6 address pool number.
Prefix-pool	Prefix pool referenced by the address pool. If no referenced prefix pool is specified, this field displays **Not configured**.

# Display detailed information about a specified address pool.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Static bindings:
    DUID: 0003000100E0FC000001
    IAID: 0000003F
    Prefix: 2::/64
      preferred lifetime 604800, valid lifetime 2592000
  Prefix pool: 1
    preferred lifetime 201600, valid lifetime 864000
  DNS server address:
    2::2
    2::3
  Domain name: aaa.com
  SIP server address:
    5::1
  SIP server domain name:
    bbb.com
```

Table 42 Command output

Field	Description
DHCPv6 pool	DHCPv6 address pool number.
Static bindings	Static prefix information configured in the address pool. If no static prefix is configured, this field is not displayed.
DUID	Client DUID.
IAID	Client IAID. If the IAID is not configured, this field displays **Not configured**.
Prefix	IPv6 address prefix.
preferred lifetime	Preferred lifetime of the prefix, in seconds.
valid lifetime	Valid lifetime of the prefix, in seconds.
Prefix Pool	Prefix pool referenced by the address pool. If no prefix pool is referenced, this field is not displayed.
DNS server address	DNS server address. If no DNS server address is configured, this field is not displayed.
Domain name	Domain name. If no domain name is configured, this field is not displayed.
SIP server address	SIP server address. If no SIP server address is configured, this field is not displayed.
SIP server domain name	Domain name of the SIP server. If no domain name of the SIP server is configured, this field is not displayed.

display ipv6 dhcp prefix-pool

Syntax

display ipv6 dhcp prefix-pool [*prefix-pool-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

prefix-pool-number: Displays details about the prefix pool specified by the prefix pool number. If no prefix pool number is specified, the brief information of all prefix pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp prefix-pool** to display prefix pool information.

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 details about the specified prefix pool.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64
Assigned length: 70
Total prefix number: 64
Available: 64
In-use: 0
Static: 0
```

Table 43 Command output

Field	Description
Prefix-pool	Prefix pool number
Prefix	Prefix contained in the prefix pool
Available	Number of idle prefixes
In-use	Number of assigned prefixes
Static	Number of static prefixes
Assigned length	Length of prefixes to be assigned
Total prefix number	Total number of prefixes

display ipv6 dhcp server

Syntax

display ipv6 dhcp server [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 server information of the interface specified by interface type and number. If no interface is specified, the DHCPv6 server information of all interfaces is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server** to display DHCPv6 server information.

Examples

# Display the DHCPv6 server information of all interfaces.

```
<Sysname> display ipv6 dhcp server
DHCPv6 server status: Enabled
Interface             Pool
Vlan-interface2       1
Vlan-interface3       2
```

# Display the DHCPv6 server information on the specified interface.

```
<Sysname> display ipv6 dhcp server interface vlan-interface 2
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

Table 44 Command output

Field	Description
DHCPv6 server status	DHCPv6 server status, which can be **Enabled** or **Disabled**.
Interface	Interface on which the DHCPv6 server is enabled
Pool	Address pool applied to the interface
Using pool	Address pool applied to the interface
Preference value	Server priority in the DHCPv6 Advertise message. The value ranges from 0 to 255.
Allow-hint	Support for desired prefix assignment. The status can be **Enabled** or **Disabled**.
Rapid-commit	Support for rapid prefix assignment. The status can be **Enabled** or **Disabled**.

display ipv6 dhcp server pd-in-use

Syntax

display ipv6 dhcp server pd-in-use { **all** | **pool** *pool-number* | **prefix** *prefix/prefix-len* | **prefix-pool** *prefix-pool-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all PD information.

pool *pool-number*: Displays the PD information of the address pool specified by the pool number.

prefix *prefix/prefix-len*: Displays the PD information of the specified prefix. The *prefix/prefix-len* indicates the IPv6 prefix and prefix length. The value of the prefix length ranges from 1 to 128.

prefix-pool *prefix-pool-number*: Displays the PD information of the prefix pool specified by the prefix pool number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server pd-in-use** to display PD information.

The PD information generated for static prefixes is not displayed when you display the PD information of a specific prefix pool.

Examples

# Display all PD information.

```
<Sysname> display ipv6 dhcp server pd-in-use all
Total number = 3
Prefix                                      Type       Pool Lease-expiration
2:1::/24                                    Auto(O)    1    Jul 10 2008 19:45:01
1:1::/64                                    Static(F) 2    Not available
1:2::/64                                    Static(O) 3    Oct  9 2008 09:23:31
```

# Display the PD information of the specified address pool.

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Total number = 2
Prefix                                      Type       Pool Lease-expiration
2:1::/24                                    Auto(O)    1    Jul 10 2008 22:22:22
3:1::/64                                    Static(C) 1    Jan  1 2008 11:11:11
```

# Display the PD information of the specified prefix pool.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix-pool 1
Total number = 1
Prefix                                      Type       Pool Lease-expiration
2:1:1:2::/64                                Auto(C)    2    Jan  1 2008 14:45:56
```

# Display the PD information of the specified prefix.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Prefix pool: 1
Client: FE80::C800:CFF:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  Prefix: 2:1::/24
  Preferred lifetime 400, valid lifetime 500
  expires at Jul 10 2008 09:45:01 (288 seconds left)
```

Table 45 Command output

Field	Description
Total number	Total number of PDs.
Prefix	Assigned IPv6 prefix.
Type	PD type: • **Static(F)**—Generated for the static prefix that has not been assigned to the client, and is also called the ineffective static PD. • **Static(O)**—Temporarily generated for the static prefix to be assigned when the server receives a Solicit message from the corresponding client. • **Static(C)**—Generated for the static prefix that is officially assigned. • **Auto(O)**—Temporarily generated for the prefix selected from a prefix pool after the server receives a Solicit message from the client. • **Auto(C)**—Generated for the prefix to be assigned officially after the server receives a Request message, or the server supporting rapid assignment receives the Solicit message containing a Rapid Commit option.
Pool	Address pool to which the PD belongs.
Lease-expiration	Lease expiration time. If the lease expires after the year 2100, this field displays **after 2100**. For the ineffective static PD, this field displays **Not available**.
Prefix Pool	Prefix pool to which the PD belongs. For the static PD, this field displays null.
Client	IPv6 address of the DHCPv6 client. For the ineffective static PD, this field displays null.
DUID	Client DUID
IAID	Client IAID. For the ineffective static PD with no IAID configured, this field displays null.
preferred lifetime	Preferred lifetime of the prefix, in seconds.
valid lifetime	Valid lifetime of the prefix, in seconds.
expires at	Lease expiration time. If the lease expires after the year 2100, this field displays **expires after 2100**.

display ipv6 dhcp server statistics

Syntax

display ipv6 dhcp server statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server statistics** to display packet statistics on the DHCPv6 server.

Examples

# Display packet statistics on the DHCPv6 server.

```
<Sysname> display ipv6 dhcp server statistics
Packets received     :  0
  SOLICIT            :  0
  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 46 Command output

Field	Description
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
Packets dropped	Number of packets discarded
Packets sent	Number of messages sent out from the DHCPv6 server. The message types include: • ADVERTISE • RECONFIGURE • REPLY • RELAY-REPLY

dns-server

Syntax

dns-server *ipv6-address*

undo dns-server *ipv6-address*

View

DHCPv6 address pool view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

Description

Use **dns-server** to specify a DNS server for the client.

Use **undo dns-server** to remove the specified DNS server.

No DNS server address is specified by default.

You can configure multiple DNS server addresses by using the **dns-server** command repeatedly.

The precedence of the specified DNS servers depends on the configuration sequence. The formerly specified DNS server takes precedence over the latter one.

NOTE:

You can configure up to eight DNS servers in an address pool.

Examples

# Specify the DNS server address to be assigned to the client as 2:2::3.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCPv6 address pool view

Default level

2: System level

Parameters

domain-name: Domain name, a string of 1 to 50 characters.

Description

Use **domain-name** to configure the domain name for the client.

Use **undo domain-name** to remove the configuration.

By default, no domain name is configured for the client.

You can configure only one domain name in an address pool.

If you repeatedly use the **domain-name** command, the latest configuration overwrites the previous one.

Examples

# Configure the domain name to be assigned to the client as aaa.com.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

ds-lite address

Syntax

ds-lite address *ipv6-address*

undo ds-lite address

View

DHCPv6 address pool view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the Address Family Translation Router (AFTR).

Description

Use **ds-lite address** to specify the address of the AFTR.

Use **undo ds-lite address** to delete the address of the AFTR.

The address of the AFTR is not specified by default.

You can specify only one AFTR address for an address pool. The latest setting overrides the previous one.

Examples

# Specify the AFTR address as 2::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] ds-lite address 2::1
```

ipv6 dhcp dscp (for DHCPv6 server)

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameter

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 server.

Use **undo ipv6 dhcp dscp** to restore the default.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

# Set the DSCP value to 30 in DHCPv6 packets sent by the DHCPv6 server.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 dhcp pool

Syntax

ipv6 dhcp pool *pool-number*

undo ipv6 dhcp pool *pool-number*

View

System view

Default level

2: System level

Parameters

pool-number: Specifies an address pool number.

Description

Use **ipv6 dhcp pool** to create a DHCPv6 address pool and enter DHCPv6 address pool view, or enter DHCPv6 address pool view if the specified address pool already exists.

Use **undo ipv6 dhcp pool** to remove the address pool.

No DHCPv6 address pool is configured by default.

Examples

# Create DHCPv6 address pool 1 and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1]
```

ipv6 dhcp prefix-pool

Syntax

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

undo ipv6 dhcp prefix-pool *prefix-pool-number*

View

System view

Default level

2: System level

Parameters

prefix-pool-number: Specifies a prefix pool number.

prefix *prefix/prefix-len*: Specifies the prefix contained in the specified prefix pool. The *prefix* indicates the IPv6 prefix. The *prefix-len* indicates the prefix length, in the range of 1 to 128.

assign-len *assign-len*: Specifies the length of the prefix assigned. The value ranges from 1 to 128. The *assign-len* must be higher than or equal to the *prefix-len*, and the difference between them must be less than or equal to 16.

Description

Use **ipv6 dhcp prefix-pool** to create a prefix pool and specify the prefix and the length of the prefix assigned.

Use **undo ipv6 dhcp prefix-pool** to remove the prefix pool.

No prefix pool is configured by default.

The prefix ranges of the prefix pools cannot overlap.

You cannot modify an existing prefix pool.

Removing a prefix pool clears all PDs assigned from the prefix pool.

Examples

# Create prefix pool 1 that contains the prefix 2001:0410::/32 and specify the length of prefixes to be assigned as 42. Prefix pool 1 can assign 1024 prefixes in the range of 2001:0410::/42 to 2001:0410:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

ipv6 dhcp server apply pool

Syntax

ipv6 dhcp server apply pool *pool-number* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *

undo ipv6 dhcp server apply pool

View

Interface view

Default level

2: System level

Parameters

pool-number: Specifies an address pool number.

allow-hint: Configure the server to support desired prefix assignment. If this keyword is not specified, the server does not support assignment of desired prefixes.

preference *preference-value*: Specifies the server priority in Advertise messages, in the range of 0 to 255. The default value is 0. A higher value indicates a higher priority.

rapid-commit: Configure the server to support rapid prefix assignment. If this keyword is not specified, the server does not support rapid prefix assignment.

Description

Use **ipv6 dhcp server apply pool** to apply a DHCPv6 address pool to the interface.

Use **undo ipv6 dhcp server apply pool** to remove the configuration.

No address pool is applied to an interface by default.

Upon receiving a request from a DHCPv6 client on an interface, the DHCPv6 server selects a prefix from the address pool applied to the interface and assigns it to the client.

With the **allow-hint** keyword specified, the server assigns the desired prefix to the requesting client. If the desired prefix is not included in the assignable prefix pool of the interface, or is already assigned to another client, the server ignores the desired prefix and assigns the client a prefix from the idle prefixes.

An interface cannot serve as a DHCPv6 server and DHCPv6 relay agent at the same time. HP does not recommend enabling the DHCPv6 server and DHCPv6 client on the same interface.

You can apply a non-existing address pool to an interface. However, the server cannot assign any prefix or other configuration information from the address pool until the address pool is created.

You cannot modify the address pool applied to an interface or parameters such as the server priority by using the **ipv6 dhcp server apply pool** command. You need to remove the applied address pool before you can apply another address pool to the interface or modify parameters such as the server priority.

NOTE:

Only one address pool can be applied to an interface.

Examples

# Apply prefix pool 1 to VLAN-interface 2, configure the server to support desired prefix assignment and rapid prefix assignment, and set the highest priority of 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

ipv6 dhcp server enable

Syntax

ipv6 dhcp server enable

undo ipv6 dhcp server enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp server enable** to enable the DHCPv6 server.

Use **undo ipv6 dhcp server enable** to disable the DHCPv6 server.

By default, the DHCPv6 server is disabled.

Other DHCPv6 server related configuration is effective only when the DHCPv6 server is enabled.

Examples

# Enable the DHCPv6 server.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server enable
```

prefix-pool

Syntax

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo prefix-pool

View

DHCPv6 address pool view

Default level

2: System level

Parameters

prefix-pool-number: Prefix pool number.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime of prefixes to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 604800 seconds, that is, seven days.

valid-lifetime *valid-lifetime*: Specifies the valid lifetime of the prefixes to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 2592000 seconds, that is, 30 days. The valid lifetime must be greater than or equal to the preferred lifetime.

Description

Use **prefix-pool** to apply a prefix pool to the DHCPv6 address pool, so that the DHCPv6 server can dynamically select a prefix from the prefix pool and assign it to the client.

Use **undo prefix-pool** to remove the configuration.

No prefix pool is referenced by an address pool by default.

Only one prefix pool can be referenced by an address pool.

A non-existing prefix pool can be referenced by an address pool. However, no prefix is available in the prefix pool for dynamic prefix assignment until the prefix pool is created.

You cannot modify the prefix pool referenced by an address pool, or the preferred lifetime or valid lifetime by using the **prefix-pool** command. You need to remove the configuration before you can have another prefix pool referenced by the address pool, or modify the preferred lifetime and valid lifetime.

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 1 to address pool 1, and set the valid lifetime to three days, the preferred lifetime to one day.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1 preferred-lifetime 86400 valid-lifetime 259200
```

reset ipv6 dhcp server pd-in-use

Syntax

reset ipv6 dhcp server pd-in-use { **all** | **pool** *pool-number* | **prefix** *prefix/prefix-len* }

View

User view

Default level

2: System level

Parameters

all: Clears all the PD information.

pool *pool-number*: Clears the PD information of the address pool specified by the pool number.

prefix *prefix/prefix-len*: Clears the PD information of the specified prefix. The *prefix/prefix-len* indicates the IPv6 prefix and prefix length. The value of the prefix length ranges from 1 to 128.

Description

Use **reset ipv6 dhcp server pd-in-use** to clear the PD information of the DHCPv6 server.

After the PD information of assigned static prefixes is removed, the PDs become ineffective static PDs.

Examples

# Clear all the PD information.

```
<Sysname> reset ipv6 dhcp server pd-in-use all
```

# Clear the PD information of the specified address pool.

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

# Clear the PD information of the specified prefix.

```
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

reset ipv6 dhcp server statistics

Syntax

reset ipv6 dhcp server statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset ipv6 dhcp server statistics** to remove packet statistics on the DHCPv6 server.

Examples

# Clear packet statistics on the DHCPv6 server.

```
<Sysname> reset ipv6 dhcp server statistics
```

sip-server

Syntax

sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

undo sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

View

DHCPv6 address pool view

Default level

2: System level

Parameters

address *ipv6-address*: Specifies the IPv6 address of a SIP server.

domain-name *domain-name*: Specifies the domain name of a SIP server. The domain name is a string of 1 to 50 characters.

Description

Use **sip-server** to configure the IPv6 address or domain name of a SIP server for the client.

Use **undo sip-server** to remove the configuration.

No SIP server address or domain name is specified by default.

You can configure up to eight SIP server addresses and eight SIP server domain names in an address pool. The priorities of the specified SIP servers depend on the configuration sequence. The formerly specified SIP server takes precedence over the latter one.

If you repeatedly use the **sip-server** command, the last configuration does not overwrite the previous one.

Examples

# Specify the SIP server address as 2:2::4 for the client.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

# Specify the domain name of the SIP server as bbb.com for the client.

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

static-bind prefix

Syntax

static-bind prefix *prefix/prefix-len* **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo static-bind prefix *prefix/prefix-len*

View

DHCPv6 address pool view

Default level

2: System level

Parameters

prefix/prefix-len: Static prefix and prefix length.

duid *duid*: Client DUID. The value is an even hexadecimal number, in the range of 2 to 256.

iaid *iaid*: Client IAID. The value is a hexadecimal number in the range of 0 to FFFFFFFF. If no IAID is specified, the server does not match against the client IAID for prefix assignment.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime of the prefix to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 604800 seconds, that is, seven days.

valid-lifetime *valid-lifetime*: Specifies the valid lifetime of the prefix to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 2592000 seconds, that is, 30 days. The valid lifetime must be greater than or equal to the preferred lifetime.

Description

Use **static-bind prefix** to configure a static prefix.

Use **undo static-bind prefix** to remove a static prefix.

No static prefix is configured by default.

After a static prefix is bound to a client, the configuration cannot be modified. You need to delete the static prefix before you can bind the prefix to another client.

Examples

# Configure static prefix 2001:0410::/35 in address pool 1, and specify the DUID as 00030001CA0006A400, the IAID as A1A1A1A1, the preferred lifetime as one day, and the valid lifetime as three days.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid
A1A1A1A1 preferred-lifetime 86400 valid-lifetime 259200
```

DHCPv6 relay agent configuration commands

display ipv6 dhcp relay server-address

Syntax

display ipv6 dhcp relay server-address { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all DHCPv6 server address information.

interface *interface-type interface-number*: Displays DHCPv6 server address information of the specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp relay server-address** to display information about DHCPv6 server addresses specified on the DHCPv6 relay agent.

Examples

# Display all the DHCPv6 server address information.

```
<Sysname> display ipv6 dhcp relay server-address all
Interface: Vlan2
Server address(es)                              Output Interface
1::1
FF02::1:2                                       Vlan4

Interface: Vlan3
Server address(es)                              Output Interface
1::1
FF02::1:2                                       Vlan4
```

# Display DHCPv6 server address information of VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan2
Server address(es)                              Output Interface
1::1
```

```
FF02::1:2                                    Vlan4
```

Table 47 Command output

Field	Description
Interface	Interface that serves as the DHCPv6 relay agent
Server address(es)	DHCPv6 server addresses specified on the interface
Output Interface	Outgoing interface of DHCPv6 packets

display ipv6 dhcp relay statistics

Syntax

display ipv6 dhcp relay statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp relay statistics** to display packet statistics on the DHCPv6 relay agent.

Related commands: **reset ipv6 dhcp relay statistics**.

Examples

# Display packet statistics on the DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped              :  4
    Error                    :  4
    Excess of rate limit     :  0
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
```

Table 48 Command output

Field	Description
Packets dropped	Number of discarded packets
Error	Number of discarded error packets
Excess of rate limit	Number of packets discarded due to excess of rate limit
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

ipv6 dhcp dscp (for DHCPv6 relay agent)

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 relay agent.

Use **undo ipv6 dhcp dscp** to restore the default.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

# Set the DSCP value to 30 in DHCPv6 packets sent by the DHCPv6 relay agent.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 dhcp relay server-address

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*]

View

Interface view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the DHCPv6 server.

interface *interface-type interface-number*: Specifies an outgoing interface for DHCPv6 packets.

Description

Use **ipv6 dhcp relay server-address** to enable DHCPv6 relay agent on the interface and specify a DHCPv6 server.

Use **undo ipv6 dhcp relay server-address** to remove the DHCPv6 server from the interface.

By default, DHCPv6 relay agent is disabled and no DHCPv6 server is specified on the interface.

Upon receiving a request from a DHCPv6 client, the interface that operates as a DHCPv6 relay agent encapsulates the request into a Relay-forward message and forwards the message to the specified DHCPv6 server, which then assigns an IPv6 address and other configuration parameters to the DHCPv6 client.

Executing the **ipv6 dhcp relay server-address** command repeatedly can specify multiple DHCPv6 servers, and up to eight DHCP servers can be specified for an interface. After receiving requests from DHCPv6 clients, the DHCPv6 relay agent forwards the requests to all the specified DHCPv6 servers.

If the DHCPv6 server address is a link-local address or link-scoped multicast address on the local link, you must specify an outgoing interface. If no outgoing interface is specified, DHCPv6 packets may fail to be forwarded to the DHCPv6 server.

After you remove all the specified DHCPv6 servers from an interface with the **undo ipv6 dhcp relay server-address** command, DHCPv6 relay agent is disabled on the interface.

An interface cannot serve as a DHCPv6 client and DHCPv6 relay agent at the same time.

Related commands: **display ipv6 dhcp relay server-address**.

Examples

# Enable DHCPv6 relay agent on VLAN-interface 2, and specify the DHCPv6 server address as 2001:1::3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

reset ipv6 dhcp relay statistics

Syntax

reset ipv6 dhcp relay statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset ipv6 dhcp relay statistics** to clear packets statistics on the DHCPv6 relay agent.

After this command is executed, the packets statistics is displayed as 0 when you use the **display ipv6 dhcp relay statistics** command.

Related commands: **display ipv6 dhcp relay statistics**.

Examples

# Clear packet statistics on the DHCPv6 relay agent.

```
<Sysname> reset ipv6 dhcp relay statistics
```

DHCPv6 client configuration commands

display ipv6 dhcp client

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 client information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp client** to display DHCPv6 client information.

With no parameters specified, the DHCPv6 client information of all the interfaces is displayed.

Examples

# Display the DHCPv6 client information of VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2 is in stateless DHCPv6 client mode
State is OPEN
Preferred Server:
    Reachable via address    :  FE80::213:7FFF:FEF6:C818
    DUID                     :  0003000100137ff6c818
    DNS servers              :  1:2:3::5
                                1:2:4::7
    Domain names             :  abc.com
```

Table 49 Command output

Field	Description
in stateless DHCPv6 client mode	Indicates the client is in the stateless DHCPv6 configuration mode.
State is OPEN	Current state of the DHCPv6 client: • **INIT**—After enabled, the DHCPv6 client enters the INIT state. • **IDLE**—After receiving an RA message with the "M" flag set to 0 and "O" flag set to 1 and enabled with stateless DHCPv6, the DHCPv6 client enters the IDLE state. • **INFO-REQUESTING**—The DHCPv6 client is requesting configuration information. • **OPEN**—The DHCPv6 client successfully obtained configuration parameters and completed stateless configuration based on the obtained parameters.
Preferred Server	Information about the DHCPv6 server selected by the DHCPv6 client.
Reachable via address	Reachable address, which is the link local address of the DHCPv6 server or relay agent.
DUID	DHCP unique identifier (DUID) of the DHCPv6 server.
DNS servers	DNS server address sent by the DHCPv6 server.

Field	Description
Domain names	Domain name information sent by the DHCPv6 server.

display ipv6 dhcp client statistics

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 client statistics of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp client statistics** to display DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all the interfaces is displayed.

Related commands: **reset ipv6 dhcp client statistics**.

Examples

# Display DHCPv6 client statistics of 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
         Confirm              :  0
         Renew                :  0
         Rebind               :  0
         Information-request :  5
         Release              :  0
```

```
        Decline             :  0
```

Table 50 Command output

Field	Description
Interface	Interface that servers 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
Confirm	Number of sent confirm 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

ipv6 dhcp client dscp

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp client dscp** to set the DSCP value in DHCPv6 packets sent by the DHCPv6 client.

Use **undo ipv6 dhcp client dscp** to restore the default value.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

# Set the DSCP value to 30 in the DHCPv6 packets sent by the DHCPv6 client.

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

```
[Sysname] ipv6 dhcp client dscp 30
```

reset ipv6 dhcp client statistics

Syntax

reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears DHCPv6 client statistics of a specified interface.

Description

Use **reset ipv6 dhcp client statistics** to clear DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all the interfaces is cleared.

After this command is executed, the packets statistics is displayed as 0 when you use the **display ipv6 dhcp client statistics** command.

Related commands: **display ipv6 dhcp client statistics**.

Examples

# Clear DHCPv6 client statistics of all the interfaces.

```
<Sysname> reset ipv6 dhcp client statistics
```

DHCPv6 snooping configuration commands

display ipv6 dhcp snooping trust

Syntax

display ipv6 dhcp snooping trust [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp snooping trust** to display DHCPv6 snooping trusted ports.

Examples

# Display DHCPv6 snooping trusted ports.

```
<Sysname> display ipv6 dhcp snooping trust
 Trusted ports include:
 GigabitEthernet1/0/1
 GigabitEthernet1/0/2
```

display ipv6 dhcp snooping user-binding

Syntax

display ipv6 dhcp snooping user-binding { *ipv6-address* | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Displays DHCPv6 snooping entries of the specified IPv6 address.

dynamic: Displays all DHCPv6 snooping entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp snooping user-binding** to display DHCPv6 snooping entries.

Examples

# Display all DHCPv6 snooping entries.

```
<Sysname> display ipv6 dhcp snooping user-binding dynamic
IPv6 Address                   MAC Address    Lease      VLAN Interface
============================== ============== ========== ==== ==================
2::1                           00e0-fc00-0006 286        1    GigabitEthernet1/0/1
---   1 DHCPv6 snooping item(s) found   ---
```

Table 51 Command output

Field	Description
IPv6 Address	IPv6 address in the DHCPv6 snooping entry.
MAC Address	MAC address in the DHCPv6 snooping entry.

Field	Description
Lease	Remaining lease of the DHCPv6 snooping entry, in seconds.
VLAN	VLAN to which the interface belongs.
Interface	Interface through which the DHCPv6 client is connected.

ipv6 dhcp snooping enable

Syntax

ipv6 dhcp snooping enable

undo ipv6 dhcp snooping enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping enable** to enable DHCPv6 snooping globally.

Use **undo ipv6 dhcp snooping enable** to disable DHCPv6 snooping globally.

By default, global DHCPv6 snooping is disabled.

After DHCPv6 snooping is enabled in system view, the DHCPv6 snooping device discards DHCPv6 reply messages received by an untrusted port if any, and does not record these DHCPv6 snooping entries.

Examples

# Enable DHCPv6 snooping globally.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

ipv6 dhcp snooping max-learning-num

Syntax

ipv6 dhcp snooping max-learning-num *number*

undo ipv6 dhcp snooping max-learning-num

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of DHCPv6 snooping entries an interface can learn, ranging from 0 to 4096.

Description

Use **ipv6 dhcp snooping max-learning-num** to configure the maximum number of DHCPv6 snooping entries an interface can learn.

Use **undo ipv6 dhcp snooping max-learning-num** to restore the default.

By default, the number of DHCPv6 snooping entries learned by an interface is not limited.

Examples

# Set the maximum number of DHCPv6 snooping entries Layer 2 Ethernet port GigabitEthernet 1/0/1 can learn to 1000.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping max-learning-num 1000
```

ipv6 dhcp snooping trust

Syntax

ipv6 dhcp snooping trust

undo ipv6 dhcp snooping trust

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping trust** to configure a DHCPv6 trusted port.

Use **undo ipv6 dhcp snooping trust** to restore the default.

By default, all interfaces of a device with DHCPv6 snooping enabled globally are untrusted ports.

After DHCPv6 snooping is enabled, to make sure that DHCPv6 clients can obtain IPv6 addresses from an authorized DHCPv6 server, you need to configure the port that connects to the authorized DHCPv6 server as a trusted port.

Examples

# Configure Ethernet port 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
```

ipv6 dhcp snooping vlan enable

Syntax

ipv6 dhcp snooping vlan enable

undo ipv6 dhcp snooping vlan enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping vlan enable** to enable DHCPv6 snooping for a specific VLAN.

Use **undo ipv6 dhcp snooping vlan enable** to disable DHCPv6 snooping for a specific VLAN.

By default, DHCPv6 snooping is disabled for a VLAN.

After DHCPv6 snooping is enabled globally and then enabled for a VLAN, the DHCPv6 snooping device records DHCPv6 snooping entries according to the DHCPv6 packets received in the VLAN. Meanwhile, upon receiving a DHCPv6 request from a client in the VLAN, the device forwards the packet through trusted ports rather than any untrusted port in the VLAN, thus reducing network traffic.

Examples

# Enable DHCPv6 snooping for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
```

reset ipv6 dhcp snooping user-binding

Syntax

reset ipv6 dhcp snooping user-binding { *ipv6-address* | **dynamic** }

View

User view

Default level

2: System level

Parameters

ipv6-address: Clears DHCPv6 snooping entries of the specified IPv6 address.

dynamic: Clears all DHCPv6 snooping entries.

Description

Use **reset ipv6 dhcp snooping user-binding** to clear DHCPv6 snooping entries.

Examples

# Clear all DHCPv6 snooping entries.

```
<Sysname> reset ipv6 dhcp snooping user-binding dynamic
```

IPv6 DNS configuration commands

display dns ipv6 server

Syntax

display dns ipv6 server [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays IPv6 DNS server information acquired dynamically through DHCP or other protocols.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns ipv6 server** to display IPv6 DNS server information.

Examples

# Display IPv6 DNS server information.

```
<Sysname> display dns ipv6 server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IPv6 Address                              (Interface Name)
    1       S     1::1
    2       S     FE80::1                                   Vlan999
```

Table 52 Command output

Field	Description
DNS Server	Sequence number of the DNS server, which is assigned automatically by the system, starting from 1.
Type	Type of the DNS server: **S** represents a statically configured DNS server, and **D** represents a DNS server obtained dynamically through DHCP or other protocols.
IPv6 Address	IPv6 address of the DNS server.

Field	Description
Interface Name	Interface name, which is available only for a DNS server with an IPv6 link-local address configured.

display ipv6 host

Syntax

display ipv6 host [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 host** to display the mappings between host names and IPv6 addresses in the static domain name resolution table.

Related commands: **ipv6 host**.

Examples

# Display the mappings between host names and IPv6 addresses in the static domain name resolution table.

```
<Sysname> display ipv6 host
Host                    Age           Flags          IPv6Address
aaa                     0             static          2002::1
bbb                     0             static          2002::2
```

Table 53 Command output

Field	Description
Host	Host name.
Age	Time for the entry to live. **0** is displayed in the case of static configuration.
Flags	Mapping type. Static indicates a static mapping.
IPv6Address	IPv6 address of a host.

dns ipv6 dscp

Syntax

dns ipv6 dscp *dscp-value*

undo dns ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in IPv6 DNS packets, in the range of 0 to 63.

Description

Use **dns ipv6 dscp** to set the DSCP value for IPv6 DNS packets.

Use **undo dns ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 DNS packets is 0.

Examples

# Set the DSCP value to 30 in IPv6 DNS packets.

```
<Sysname> system-view
[Sysname] dns ipv6 dscp 30
```

dns server ipv6

Syntax

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View

System view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface by its type and number. When the IPv6 address of the DNS server is a link-local address, the two arguments must be specified.

Description

Use **dns server ipv6** to specify a DNS server.

Use **undo dns server ipv6** to remove the specified DNS server.

By default, no DNS server is configured.

You can configure a maximum of six DNS servers, including those with IPv4 addresses.

Examples

# Specify a DNS server at 2002::1.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

ipv6 host

Syntax

ipv6 host *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View

System view

Default level

2: System level

Parameters

hostname: Specifies the host name, a string of up to 255 characters. The character string can contain letters, numbers, underscores (_), hyphens (-), or dots (.) and must contain at least one letter.

ipv6-address: Specifies the IPv6 address.

Description

Use **ipv6 host** to configure a mapping between host name and IPv6 address.

Use **undo ipv6 host** to remove a mapping between host name and IPv6 address.

No mappings are created by default.

Each host name can correspond to only one IPv6 address. The IPv6 address you last assign to the host name will overwrite the previous one if there is any.

Related commands: **display ipv6 host**.

Examples

# Configure the mapping between a host name and an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

Index

Contents

Basic IP routing commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

display ip routing-table

Syntax

display ip routing-table [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed routing table information, including inactive routes. With this keyword absent, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table** to display brief information about active routes in the routing table.

This command displays brief information about a routing table, with a routing entry contained in one line. The information displayed includes destination IP address/mask length, protocol, priority, cost, next hop, and outbound interface. This command displays only the optimal routes in use.

Use **display ip routing-table verbose** to display detailed information about all routes in the routing table.

This command displays detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples

# Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
         Destinations : 6       Routes : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.2.0/24          Direct 0    0            1.1.2.1         Vlan11
1.1.2.1/32          Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
192.168.0.0/24      Direct 0    0            192.168.0.1     Vlan1
192.168.0.1/32      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 presents the route
Pre	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

# Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
Routing Tables: Public
         Destinations : 6       Routes : 6

  Destination: 1.1.2.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 1.1.2.1          Interface: Vlan-interface11
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active Adv             Age: 06h46m22s
          Tag: 0

  Destination: 1.1.2.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 127.0.0.1        Interface: InLoopBack0
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active NoAdv           Age: 06h46m22s
          Tag: 0

  Destination: 127.0.0.0/8
```

```
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 127.0.0.1        Interface: InLoopBack0
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active NoAdv           Age: 06h46m36s
          Tag: 0

  Destination: 127.0.0.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 127.0.0.1        Interface: InLoopBack0
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active NoAdv           Age: 06h46m37s
          Tag: 0

  Destination: 192.168.0.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 192.168.0.1      Interface: Vlan-interface1
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active Adv             Age: 06h46m35s
          Tag: 0

  Destination: 192.168.0.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
 IpPrecedence:                    QosLcId:
      NextHop: 127.0.0.1        Interface: InLoopBack0
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active NoAdv           Age: 06h46m35s
          Tag: 0
```

Displayed first are statistics for the whole routing table, followed by a detailed description of each route (in sequence).

Table 2 Command output

Field	Description
Destination	Destination address/mask length.
Protocol	Protocol that presents the route.
Process ID	Process ID.
Preference	Priority of the route.
Cost	Cost of the route.
IpPrecedence	IP precedence.
QosLcId	QoS-local ID.
NextHop	Address of the next hop on the route.
Interface	Outbound interface for packets to be forwarded along the route.
BkNextHop	Backup next hop.
BkInterface	Backup outbound interface.
RelyNextHop	Next hop address obtained through routing recursion.
Neighbor	Neighboring address determined by routing protocol.
Tunnel ID	Tunnel ID.
Label	Label.
BKTunnel ID	Backup tunnel ID.
BKLabel	Backup label.

Field	Description
State	Route status: - **Active**—This is an active unicast route. - **Adv**—This route can be advertised. - **Delete**—This route is deleted. - **Gateway**—This is an indirect route. - **Holddown**—Number of holddown routes. - **Int**—The route was discovered by an Interior Gateway Protocol (IGP). - **NoAdv**—The route is not advertised when the router advertises routes based on policies. - **NotInstall**—Among routes to a destination, the route with the highest priority is installed into the core routing table and advertised. A NotInstall route cannot be installed into the core routing table but can be advertised. - **Reject**—The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the sources of the dropped packets. The Reject routes are usually used for network testing. - **Static**—A static route is not lost when you perform the save operation and then restart the router. Routes configured manually are marked as **static**. - **Unicast**—Unicast routes. - **Inactive**—Inactive routes. - **Invalid**—Invalid routes. - **WaitQ**—The route is the WaitQ during route recursion. - **TunE**—Tunnel. - **GotQ**—The route is in the GotQ during route recursion.
Age	Time for which the route has been in the routing table, in the sequence of hour, minute, and second from left to right.
Tag	Route tag.

display ip routing-table *ip-address*

Syntax

display ip routing-table *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display ip routing-table *ip-address1* { *mask* | *mask-length* } *ip-address2* { *mask* | *mask-length* } [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Specifies the destination IP address, in dotted decimal format.

mask | *mask-length*: Specifies the IP address mask, in dotted decimal format or represented by an integer in the range of 0 to 32.

longer-match: Displays the route with the longest mask.

verbose: Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table** *ip-address* to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*
    - The system ANDs the input destination IP address with the subnet mask in each route entry.
    - The system ANDs the destination IP address in each route entry with its own subnet mask.
    - If the two operations yield the same result for an entry and this entry is active, it is displayed.
- **display ip routing-table** *ip-address mask*
    - The system ANDs the input destination IP address with the input subnet mask.
    - The system ANDs the destination IP address in each route entry with the input subnet mask.
    - If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.
    - Only route entries that exactly match the input destination address and mask are displayed.
- **display ip routing-table** *ip-address* **longer-match**
    - The system ANDs the input destination IP address with the subnet mask in each route entry.
    - The system ANDs the destination IP address in each route entry with its own subnet mask.
    - If the two operations yield the same result for multiple entries that are active, the one with the longest mask length is displayed.
- **display ip routing-table** *ip-address mask* **longer-match**
    - The system ANDs the input destination IP address with the input subnet mask.
    - The system ANDs the destination IP address in each route entry with the input subnet mask.
    - If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use**display ip routing-table** *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } to display route entries with destination addresses within a specified range.

Examples

# Display route entries for the destination IP address 11.1.1.1.

```
<Sysname> display ip routing-table 11.1.1.1
Routing Table : Public
Summary Count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            0.0.0.0         NULL0
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

# Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
<Sysname> display ip routing-table 11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

# Display route entries by specifying a destination IP address and mask.

```
<Sysname> display ip routing-table 11.1.1.1 24
Routing Table : Public
Summary Count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

# Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
<Sysname> display ip routing-table 11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

# Display route entries for destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

Destination/Mask    Proto  Pre  Cost         NextHop       Interface

1.1.1.0/24          Direct 0    0            1.1.1.1       Vlan1
1.1.1.1/32          Direct 0    0            127.0.0.1     InLoop0
2.2.2.0/24          Direct 0    0            2.2.2.1       Vlan2
```

```
3.3.3.0/24          Direct 0    0            3.3.3.1       Vlan12
3.3.3.1/32          Direct 0    0            127.0.0.1     InLoop0
4.4.4.0/24          Direct 0    0            4.4.4.1       Vlan11
4.4.4.1/32          Direct 0    0            127.0.0.1     InLoop0
```

For output descriptions, see Table 1.

display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

protocol: Specifies the routing protocol. It can be **direct** and **static**.

inactive: Displays information about only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. With this argument absent, the command displays brief routing table information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table protocol** to display routing information of a specified routing protocol.

Examples

# Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
Public Routing Table : Direct
Summary Count : 6

Direct Routing Table Status : <Active>
Summary Count : 6

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0           127.0.0.1       InLoop0
```

```
127.0.0.0/8         Direct 0    0          127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0          127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0          192.168.80.10   Vlan11
192.168.80.10/32    Direct 0    0          127.0.0.1       InLoop0

Direct Routing Table Status : <Inactive>
Summary Count : 0
```

# Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static
Public Routing Table : Static
Summary Count : 2

Static Routing Table Status : <Active>
Summary Count : 0

Static Routing Table Status : <Inactive>
Summary Count : 2

Destination/Mask    Proto   Pre  Cost        NextHop      Interface
1.2.3.0/24          Static  60   0           1.2.4.5      Vlan10
3.0.0.0/8           Static  60   0           2.2.2.2      Vlan11
```

For output descriptions, see Table 1.

display ip routing-table statistics

Syntax

display ip routing-table statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table statistics** to display the route statistics of the routing table.

Examples

# Display route statistics in the routing table.

```
<Sysname> display ip routing-table statistics
```

```
Proto       route       active      added       deleted       freed
DIRECT      24          4           25          1             0
STATIC      4           1           4           0             0
Total       28          5           29          1             0
```

Table 3 Command output

Field	Description
Proto	Origin of the routes
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the router started up or the routing table was last cleared
deleted	Number of routes marked as deleted, which will be freed after a period
freed	Number of routes that got freed (got removed permanently)
Total	Total number

display ipv6 routing-table

Syntax

display ipv6 routing-table [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about both active and inactive routes. Without this keyword, only brief information about active routes is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table** to display brief IPv6 routing information, including destination IP address and prefix, protocol type, priority, metric, next hop, and outbound interface.

The command displays only active routes (the brief information about the current optimal routes).

Use **display ipv6 routing-table verbose** to display detailed information about all IPv6 routes, including both active and inactive routes. The output shows the statistics of the entire routing table, and then the detailed information of each route.

Examples

# Display brief routing table information

```
<Sysname> display ipv6 routing-table
Routing Table : Public
        Destinations : 1        Routes : 1
Destination: ::1/128                           Protocol  : Direct
NextHop    : ::1                               Preference: 0
Interface  : InLoop0                           Cost      : 0
```

Table 4 Command output

Field	Description
Destination	IPv6 address of the destination network/host
NextHop	Next hop address
Preference	Route priority
Interface	Outbound interface
Protocol	Routing protocol
Cost	Route cost

# Display detailed routing table information.

```
<Sysname> display ipv6 routing-table verbose
Routing Table : Public
         Destinations : 1        Routes : 1

 Destination  : ::1                                     PrefixLength : 128
 NextHop      : ::1                                     Preference   : 0
 IpPrecedence :                                         QosLcId      :
 RelayNextHop : ::                                      Tag          : 0H
 Neighbor     : ::                                      ProcessID    : 0
 Interface    : InLoopBack0                             Protocol     : Direct
 State        : Active NoAdv                            Cost         : 0
 Tunnel ID    : 0x0                                     Label        : NULL
 Age          : 22161sec
```

Table 5 Command output

Field	Description
Destination	IPv6 address of the destination network/host
PrefixLength	Prefix length of the address
NextHop	Next hop
Preference	Route priority
IpPrecedence	IP precedence
QosLcId	QoS-local ID
RelayNextHop	Recursive next hop
Tag	Tag of the route

Field	Description
Neighbor	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)
Cost	Cost of the route
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

display ipv6 routing-table *ipv6-address*

Syntax

display ipv6 routing-table *ipv6-address prefix-length* [**longer-match**] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display ipv6 routing-table *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the prefix length, in the range of 0 to 128.

longer-match: Displays the matched route having the longest prefix length.

ipv6-address1/*ipv6-address2*: Specifies the an IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/*prefix-length2*: Specifies the prefix length, in the range of 0 to 128.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table** *ipv6-address* to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table** *ipv6-address prefix-length*
  - The system ANDs the input destination IPv6 address with the input prefix length.
  - The system ANDs the destination IPv6 address in each route entry with the input prefix length.
  - If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.
  - Only route entries that exactly match the input destination address and prefix length are displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**
  - The system ANDs the input destination IPv6 address with the input prefix length.
  - The system ANDs the destination IPv6 address in each route entry with the input prefix length.
  - If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

Use **display ipv6 routing-table** *ipv6-address1 ipv6-address2* to display routes whose destinations fall into the specified IPv6 address range.

Examples

# Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
Routing Table: Public
Summary Count: 3

Destination: 10::/64                                     Protocol  : Static
NextHop    : ::                                          Preference: 60
Interface  : NULL0                                       Cost      : 0

Destination: 10::/68                                     Protocol  : Static
NextHop    : ::                                          Preference: 60
Interface  : NULL0                                       Cost      : 0

Destination: 10::/120                                     Protocol  : Static
NextHop    : ::                                           Preference: 60
Interface  : NULL0                                        Cost      : 0
```

# Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
Routing Tables: Public
Summary Count : 1
Destination: 10::/120                                     Protocol  : Static
NextHop    : ::                                           Preference: 60
Interface  : NULL0                                        Cost      : 0
```

# Display routes whose destinations fall into the specified IPv6 address range.

```
<Sysname> display ipv6 routing-table 100:: 64 300:: 64
```

```
Routing Table : Public
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
         Cost      : 0
```

For output description, see Table 4 .

display ipv6 routing-table protocol

Syntax

display ipv6 routing-table protocol *protocol* [**inactive** | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

protocol: Displays routes of a routing protocol, which can be **direct** and **static**.

inactive: Displays only inactive routes. Without this keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table protocol** to display IPv6 routes of a specified routing protocol.

Examples

# Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
```

```
Public Routing Table : Direct
Summary Count : 1

Direct Routing Table Status : <Active>
Summary Count : 1

Destination: ::1/128                                     Protocol  : Direct
NextHop    : ::1                                         Preference: 0
Interface  : InLoop0                                     Cost      : 0

Direct Routing Table Status : <Inactive>
Summary Count : 0
```

For output description, see Table 4.

display ipv6 routing-table statistics

Syntax

display ipv6 routing-table statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table statistics** to display IPv6 routing statistics, including total route number, added route number, and deleted route number.

Examples

# Display IPv6 routing statistics.

```
<Sysname> display ipv6 routing-table statistics
Protocol   route       active      added       deleted     freed
DIRECT     1           1           1           0           0
STATIC     3           0           3           0           0
Total      4           1           4           0           0
```

Table 6 Command output

Field	Description
Protocol	Routing protocol
route	Route number of the protocol
active	Number of active routes
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number
Total	Total number of routes

reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

View

User view

Default level

2: System level

Parameters

protocol: Clears statistics for the IPv4 routing protocol, which can be **direct** or **static**.

all: Clears statistics for all IPv4 routing protocols.

Description

Use **reset ip routing-table statistics protocol** to clear routing statistics for the routing table.

Examples

# Clear routing statistics in the routing table.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics

Syntax

reset ipv6 routing-table statistics protocol { *protocol* | **all** }

View

User view

Default level

2: System level

Parameters

protocol: Clears statistics for the routing protocol, which can be **direct** or **static**.

all: Clears statistics for all IPv6 routing protocols.

Description

Use **reset ipv6 routing-table statistics** to clear the route statistics of the routing table.

Examples

# Clear statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

Static routing configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

delete static-routes all

Syntax

delete static-routes all

View

System view

Default level

2: System level

Parameters

None

Description

Use **delete static-routes all** to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **display ip routing-table** and **ip route-static**.

Examples

# Delete all static routes on the router.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all ipv4 static routes and their configurations, you must reconfigure all
static routes
Are you sure?[Y/N]:Y
```

ip route-static

Syntax

ip route-static *dest-address* { *mask* | *mask-length* } { *next-hop-address* [**track** *track-entry-number*] | *interface-type interface-number* [*next-hop-address*] } [**preference** *preference-value*] [**permanent**] [**description** *description-text*]

undo ip route-static *dest-address* { *mask* | *mask-length* } [*next-hop-address* | *interface-type interface-number* [*next-hop-address*]] [**preference** *preference-value*]

View

System view

Default level

2: System level

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask: Specifies the mask of the IP address, in dotted decimal notation.

mask-length: Specifies the mask length, in the range of 0 to 32.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the outbound interface by its type and number. If the outbound interface is a broadcast interface, such as a VLAN interface, the next hop address must be specified.

preference *preference-value* : Specifies the preference of the static route, in the range of 1 to 255 and defaults to 60.

permanent: Specifies the route as a permanent static route. If the outgoing interface is down, the permanent static route is still active.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding **?** (question mark).

track *track-entry-number*: Associates the static route with a track entry. Use the *track-entry-number* argument to specify a track entry number, in the range of 1 to 1024.

Description

Use **ip route-static** to configure a unicast static route.

Use **undo ip route-static** to delete a unicast static route.

When you configure a unicast static route, follow these 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 will be used for forwarding a packet if no route is available for the packet in the routing table.
- Implement different routing policies by tuning route preference. For example, to enable them to back up one another, assign different preferences to them.
- Specify the outbound interface or the next hop address of the static route as needed. The next hop address cannot be the IP address of a local interface; otherwise, the route configuration will not take effect. If the outbound interface supports network address-to-link layer address resolution or is a point-to-point interface, you may specify only the interface or the next hop address.
    - If the outbound interface is a Null 0 interface, no next hop address is required.
    - If you specify a broadcast interface (such as a VLAN interface) as the outbound interface for a static route, you must specify the corresponding next hop of the interface at the same time.

The next hop address cannot be the IP address of a local interface (such as a VLAN interface). Otherwise, the static route does not take effect.

If a static route needs route recursion, the associated track entry must monitor the next hop of the recursive route instead of that of the static route. Otherwise, a valid route may be mistakenly considered invalid.

Do not specify the **permanent** keyword together with the **track** keyword.

Related commands: **display ip routing-table** and **ip route-static default-preference**.

Examples

# Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, and description information is **for internet & intranet**.

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

```
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 description for internet & intranet
```

ip route-static default-preference

Syntax

ip route-static default-preference *default-preference-value*

undo ip route-static default-preference

View

System view

Default level

2: System level

Parameters

default-preference-value: Specifies the default preference for static routes, in the range of 1 to 255.

Description

Use **ip route-static default-preference** to configure the default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

By default, the default preference of static routes is 60.

If no preference is specified when configuring a static route, the default preference is used.

When the default preference is re-configured, it applies only to newly added static routes.

Related commands: **display ip routing-table** and **ip route-static**.

Examples

# Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

IPv6 static routing configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

delete ipv6 static-routes all

Syntax

delete ipv6 static-routes all

View

System view

Default level

2: System level

Parameters

None.

Description

Use **delete ipv6 static-routes all** to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **ipv6 route-static** and **display ipv6 routing-table**.

Examples

# Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all ipv6 static routes and their configurations, you must reconfigure all
static routes
Are you sure?[Y/N]Y
```

ipv6 route-static

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference-value*]

View

System view

Default level

2: System level

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, such as an NBMA interface or broadcast interface (for example, a VLAN interface), the next hop address must be specified.

nexthop-address: Specifies the next hop IPv6 address.

preference *preference-value*: Specifies the route preference value, in the range of 1 to 255. The default is 60.

Description

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

If you specify a broadcast interface, such as a VLAN interface, as the output interface for a static route, you must specify the next hop address.

Related commands: **delete ipv6 static-routes all** and **display ipv6 routing-table**.

Examples

# Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

Index

Contents

IGMP snooping configuration commands

display igmp-snooping group

Syntax

display igmp-snooping group [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IGMP snooping group information in the specified VLAN, where the *vlan-id* argument is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the IGMP snooping group information in all VLANs.

slot *slot-number*: Displays the IGMP snooping group information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed IGMP snooping group information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping group** to display IGMP snooping group information, including both dynamic entries and static entries.

Examples

# Display the detailed IGMP snooping group information in VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port(s).
            GE1/0/1                (D) ( 00:01:30 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 1 port(s).
            GE1/0/2                (D) ( 00:03:23 )
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port(s).
            GE1/0/2
```

Table 1 Command output

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: **D**—Dynamic port **S**—Static port **C**—Port copied from a (*, G) entry to an (S, G) entry **P**—Port added by PIM snooping
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: **R**—Real egress sub-VLAN under the current entry **C**—Sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port
IP group address	Address of IP multicast group
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 implies any multicast source
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of member ports

display igmp-snooping host

Syntax

display igmp-snooping host vlan *vlan-id* **group** *group-address* [**source** *source-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by IGMP snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *group-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified IGMP snooping group. The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified multicast source, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

slot *slot-number*: Displays information about the hosts tracked by IGMP snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping host** to display information about the hosts tracked by IGMP snooping.

Examples

# Display information about the hosts tracked by IGMP snooping in VLAN 2 that are in multicast group 224.1.1.1.

```
<Sysname> display igmp-snooping host vlan 2 group 224.1.1.1
VLAN(ID) : 2
  (0.0.0.0, 224.1.1.1)
    Port : GigabitEthernet1/0/1
      Host                                      Uptime          Expires
      1.1.1.1                                   00:02:20        00:00:40
      2.2.2.2                                   00:02:21        00:00:39
    Port : GigabitEthernet1/0/2
      Host                                      Uptime          Expires
      3.3.3.3                                   00:02:20        00:00:40
```

Table 2 Command output

Field	Description
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 indicates all multicast sources

Field	Description
Port	Member port
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where *timeout* means that the host has expired

display igmp-snooping statistics

Syntax

display igmp-snooping statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping statistics** to display statistics for IGMP messages learned through IGMP snooping.

Examples

# Display statistics for 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 error IGMP messages:19.
```

Table 3 Command output

Field	Description
general queries	General query messages
specific queries	Group-specific query messages
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message or messages
error IGMP messages	IGMP messages with errors

display mac-address multicast

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

mac-address: Displays the multicast MAC address entry for the specified MAC address. The MAC address can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F. A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1.

vlan *vlan-id*: Displays multicast MAC address entries for the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the static multicast MAC address entries for all VLANs.

multicast: Displays static multicast MAC address entries.

count: Displays the number of matched static multicast MAC address entries. With this argument specified, the number of matched static multicast MAC address entries is displayed, without displaying any content of the matched entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-address multicast** to display the static multicast MAC address entries.

With no parameters specified or with only **vlan**, **count**, or both of them specified, this command displays all MAC address table entries, including static multicast MAC address entries and unicast MAC address entries.

Related commands: **mac-address multicast**; **display mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

# Display the static multicast MAC address entries for VLAN 2.

```
<Sysname> display mac-address multicast vlan 2
MAC ADDR        VLAN ID   STATE            PORT INDEX             AGING TIME(s)
0100-0001-0001     2      Multicast        GigabitEthernet1/0/1            NOAGED
                                           GigabitEthernet1/0/2
                                           GigabitEthernet1/0/3
                                           GigabitEthernet1/0/4

  ---  1 mac address(es) found  ---
```

Table 4 Command output

Field	Description
MAC ADDR	MAC address.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
STATE	Status of the MAC address; multicast indicates a static multicast MAC address entry.
PORT INDEX	Outgoing ports of the multicast MAC address entry.
AGING TIME(s)	State of the aging timer. The aging timer for static multicast MAC addresses has only one state **NOAGED**, which indicates that this entry never expires.
1 mac address(es) found	One static multicast MAC address entry is found.

dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

IGMP-snooping view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for IGMP messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **dot1p-priority** to set the 802.1p precedence for IGMP messages globally.

Use **undo dot1p-priority** to restore the default.

The default 802.1p precedence for IGMP messages is 0.

Examples

# Set the 802.1p precedence for IGMP messages to 3 globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

dscp (IGMP-snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

IGMP-snooping view

Default level

2: System level

Parameters

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

Description

Use **dscp** to set the DSCP value for IGMP messages.

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

The default DSCP value in IGMP messages is 48.

Examples

# Set the DSCP value to 63 for IGMP messages.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

fast-leave (IGMP-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use **undo fast-leave** to disable fast-leave processing globally.

By default, fast-leave processing is disabled.

This command works in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping fast-leave**.

Examples

# Enable fast-leave processing in VLAN 2 globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

group-policy (IGMP-snooping view)

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

IGMP-snooping view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX or TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **group-policy** to configure a global multicast group filter, namely, to control the multicast groups that a host can join.

Use **undo group-policy** to remove the configured global multicast group filter.

By default, no global multicast group filter is configured. Namely, a host can join any valid multicast group.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **igmp-snooping group-policy**.

Examples

# Apply ACL 2000 as a multicast group filter in VLAN 2 so that hosts in this VLAN can join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

Use **host-aging-time** to configure the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command works only in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping host-aging-time**.

Examples

# Set the aging timer for dynamic member ports to 300 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

host-tracking (IGMP-snooping view)

Syntax

host-tracking

undo host-tracking

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the IGMP snooping host tracking function globally.

Use **undo host-tracking** to disable the IGMP snooping host tracking function globally.

By default, this function is disabled.

This command works only in IGMP snooping–enabled VLANs.

Related commands: **display igmp-snooping host** and **igmp-snooping host-tracking**.

Examples

# Enable the IGMP snooping host tracking function globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-tracking
```

igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping** to enable IGMP snooping globally and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable IGMP snooping globally.

By default, IGMP snooping is disabled.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping globally and enter IGMP-snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

igmp-snooping access-policy

Syntax

igmp-snooping access-policy *acl-number*

undo igmp-snooping access-policy { *acl-number* | **all** }

View

User profile view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source addresses of the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

all: Specifies all ACLs.

Description

Use **igmp-snooping access-policy** to configure a multicast user control policy.

Use **undo igmp-snooping access-policy** to remove the configuration.

By default, no user control policy is configured. Namely, a user can join any valid multicast group.

You can use this command repeatedly to configure multiple multicast user control policies.

Examples

# Create and enable a user profile named **abc** to allow users to join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] igmp-snooping access-policy 2001
[Sysname-user-profile-abc] quit
[Sysname] user-profile abc enable
```

igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority-number*

undo igmp-snooping dot1p-priority

View

VLAN view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for IGMP messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **igmp-snooping dot1p-priority** to set the 802.1p precedence for the IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

The default 802.1p precedence for the IGMP messages in a VLAN is 0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping in VLAN 2 and set the 802.1p precedence for the IGMP messages in the VLAN 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
```

igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data for a VLAN.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data for a VLAN.

By default, this function is disabled. That is, unknown multicast data is flooded.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **drop-unknown** and **igmp-snooping enable**.

Examples

# In VLAN 2, enable IGMP snooping and the function of dropping unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN.

Use **undo igmp-snooping enable** to disable IGMP snooping for a VLAN.

By default, IGMP snooping is disabled in a VLAN.

IGMP snooping must be enabled globally before it can be enabled in a VLAN.

Related commands: **igmp-snooping**.

Examples

# Enable IGMP snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on the current port or group of ports.

By default, fast-leave processing is disabled.

This command works in IGMP snooping–enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

# Enable fast-leave processing on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip { *ip-address* | **current-interface** }

undo igmp-snooping general-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

current-interface: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP general queries.

Description

Use **igmp-snooping general-query source-ip** to configure the source address of IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

# In VLAN 2, enable IGMP snooping and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

limit: Specifies the maximum number of multicast groups that a port can join. in the range of 1 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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 restore the default.

By default, the upper limit is 1000.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **igmp group-limit**.

Examples

# Specify to allow GigabitEthernet 1/0/1 in VLAN 2 to join up to 10 multicast groups.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping group-policy** to configure a multicast group filter on the current port, namely, to control the multicast groups that the hosts on the port can join.

Use **undo igmp-snooping group-policy** to remove a multicast group filter.

By default, no multicast group filter is configured on an interface. Namely, a host can join any valid multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

# Apply ACL 2000 as a multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports for a VLAN.

Use **undo igmp-snooping host-aging-time** to restore the default.

By default, the aging time of a dynamic member port is 260 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **host-aging-time** and **igmp-snooping enable**.

Examples

# Enable IGMP snooping and set the aging timer for dynamic member ports in VLAN 2 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
```

igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

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

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the simulated host will join, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the simulated host will join. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping host-join** to enable simulated joining on a port. That is, you configure the port as a simulated member host for the specified multicast group or source and group.

Use **undo igmp-snooping host-join** to remove the simulated member hosts from the specified multicast group or source and group.

By default, this function is disabled.

The **source-ip** *source-address* option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip** *source-address* option does not take effect although you can include **source-ip** *source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on the ports in this port group that belong to the specified VLAN.

Examples

# Configure GigabitEthernet 1/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface 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 host-tracking

Syntax

igmp-snooping host-tracking

undo igmp-snooping host-tracking

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping host-tracking** to enable the IGMP snooping host tracking function in a VLAN.

Use **undo igmp-snooping host-tracking** to disable the IGMP snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable IGMP snooping in the VLAN first.

Related commands: **display igmp-snooping host**, **host-tracking**, and **igmp-snooping enable**.

Examples

# Enable IGMP snooping and IGMP snooping host tracking in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-tracking
```

igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

Use **igmp-snooping last-member-query-interval** to set the IGMP last-member query interval in the VLAN.

Use **undo igmp-snooping last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

The IGMP last-member query interval determines the interval for sending IGMP group-specific queries and the maximum response delay for IGMP group-specific queries in a VLAN.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **last-member-query-interval**.

Examples

# Enable IGMP snooping and set the IGMP last-member query interval to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip { *ip-address* | **current-interface** }

undo igmp-snooping leave source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP leave messages that the IGMP snooping proxy sends, which can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP leave messages that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping leave source-ip** to configure the source IP address of the IGMP leave messages that the IGMP snooping proxy sends.

Use **undo igmp-snooping leave source-ip** to restore the default.

By default, the source IP address of the IGMP leave messages that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping leave source-ip** command also applies when the simulated host sends IGMP leave messages.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP leave messages that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

Use **igmp-snooping max-response-time** to configure the maximum response delay for IGMP general queries in the VLAN.

Use **undo igmp-snooping max-response-time** to restore the default.

By default, the maximum response delay for IGMP general queries is 10 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping query-interval**, and **max-response-time**.

Examples

# Enable IGMP snooping and set the maximum response delay for IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping overflow-replace** to enable the multicast group replacement function on the current port.

Use **undo igmp-snooping overflow-replace** to disable the multicast group replacement function.

By default, the multicast group replacement function is disabled.

This command works in IGMP snooping–enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

# Enable the multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

igmp-snooping proxying enable

Syntax

igmp-snooping proxying enable

undo igmp-snooping proxying enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping proxying enable** to enable the IGMP snooping proxying function in a VLAN.

Use **undo igmp-snooping proxying enable** to disable the IGMP snooping proxying function in a VLAN.

By default, IGMP snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping and then IGMP snooping proxying 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 proxying enable
```

igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping querier** to enable the IGMP snooping querier function.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier function.

By default, the IGMP snooping querier function is disabled.

This command takes effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan.**

Examples

# Enable IGMP snooping and the IGMP snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an interval in seconds for sending IGMP general queries. The value ranges from 2 to 300.

Description

Use **igmp-snooping query-interval** to configure the interval for sending IGMP general queries.

Use **undo igmp-snooping query-interval** to restore the default.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping max-response-time**, **igmp-snooping querier**, and **max-response-time**.

Examples

# Enable IGMP snooping and set the interval for sending IGMP general queries to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping query-interval 20
```

igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip { *ip-address* | **current-interface** }

undo igmp-snooping report source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP reports that the IGMP snooping proxy sends. The address can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP reports that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping report source-ip** to configure the source IP address of the IGMP reports that the IGMP snooping proxy sends.

Use **undo igmp-snooping report source-ip** to restore the default.

By default, the source IP address of the IGMP reports that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping report source-ip** command also applies when the simulated host sends IGMP reports.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP reports that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports in seconds. The value ranges from 1 to 1000.

Description

Use **igmp-snooping router-aging-time** to configure the aging timer for dynamic router ports for a VLAN.

Use **undo igmp-snooping router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 105 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **router-aging-time**.

Examples

# Enable IGMP snooping and set the aging timer for dynamic router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

igmp-snooping router-port-deny

Syntax

igmp-snooping router-port-deny [**vlan** *vlan-list*]

undo igmp-snooping router-port-deny [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo igmp-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

This command works in both IGMP snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified 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] igmp-snooping router-port-deny vlan 2
```

igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping source-deny** to enable multicast source port filtering.

Use **undo igmp-snooping source-deny** to disable multicast source port filtering.

By default, multicast source port filtering is disabled.

This command works in IGMP snooping–enabled VLANs.

Examples

# Enable source port filtering for multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip { *ip-address* | **current-interface** }

undo igmp-snooping special-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for IGMP group-specific queries.

current-interface: Specifies the address of the current VLAN interface as the source address of IGMP group-specific queries. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP group-specific queries.

Description

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.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

# In VLAN 2, enable IGMP snooping and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

igmp-snooping static-group

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

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

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the port joins as a static member port, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the port joins as a static member port. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 means no restriction on the multicast source.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping static-group** to configure the static (*, G) or (S, G) entry for the port, namely, to configure the port as a static member port of the specified multicast group or source-group.

Use **undo igmp-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip** *source-address* option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip** *source-address* option does not take effect although you can include **source-ip** *source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 232.1.1.1 source-ip 1.1.1.1
vlan 2
```

igmp-snooping static-router-port

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port vlan *vlan-id*

View

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

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping static-router-port** to configure the current port as a static router port.

Use **undo igmp-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

This command works in IGMP snooping–enabled VLANs.

This command does not take effect in a sub-VLAN of a multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan.**

Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 as a static router port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an IGMP snooping version, in the range of 2 to 3.

Description

Use **igmp-snooping version** to configure the IGMP snooping version.

Use **undo igmp-snooping version** to restore the default.

By default, the IGMPv2 snooping is used.

This command can take effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan**.

Examples

# Enable IGMP snooping in VLAN 2, and specify IGMPv3 snooping.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

last-member-query-interval (IGMP-snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

Use **last-member-query-interval** to set the IGMP last-member query interval globally.

Use **undo last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

The IGMP last-member query interval determines the interval for sending IGMP group-specific queries and the maximum response delay for IGMP group-specific queries.

This command works only in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping last-member-query-interval**.

Examples

# Set the IGMP last-member query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

mac-address multicast

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

In Ethernet interface view or Layer 2 aggregate interface view:

mac-address multicast *mac-address* **vlan** *vlan-id*

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

In port group view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address multicast *mac-address* **vlan** *vlan-id*

View

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

Default level

2: System level

Parameters

mac-address: Specifies a static multicast MAC address, which can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F.

A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1. The system gives a prompt if the configured static multicast MAC address conflicts with the MAC address of other protocols.

interface-list: Specifies a list of interfaces. You can specify up to **n** single interfaces, interface ranges, or combinations of both for the list. A single interface takes the form of *interface-type interface-number*. An interface range takes the form of *interface-type interface-number* **to** *interface-type interface-number*, where the end interface number must be greater than the start interface number.

vlan *vlan-id*: Specifies the VLAN to which the interface belongs. *vlan-id* is in the range of 1 to 4094. The specified VLAN must exist and the system gives a prompt if the specified interface does not belong to the VLAN.

Description

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

By default, no static multicast MAC address entry is configured.

If **multicast** is not specified when using the **undo mac-address multicast** command, all MAC address entries (including static multicast MAC address entries and unicast MAC address entries) are deleted.

Related commands: **display mac-address multicast**; **mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

# Configure a static multicast MAC address entry with the MAC address of 0100-0001-0001 and outgoing interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-0001-0001 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5 vlan 2
```

# Configure a static multicast MAC address entry with the MAC address of 0100-0001-0001 in interface view of GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

max-response-time (IGMP-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

Use **max-response-time** to set the maximum response delay for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

This command works only in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping max-response-time** and **igmp-snooping query-interval**.

Examples

# Set the maximum response delay for IGMP general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

overflow-replace (IGMP-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **overflow-replace** to enable the multicast group replacement function globally.

Use **undo overflow-replace** to disable the multicast group replacement function globally.

By default, the multicast group replacement function is disabled.

This command works in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping overflow-replace**.

Examples

# Enable the multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

report-aggregation (IGMP-snooping view)

Syntax

report-aggregation

undo report-aggregation

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

This command works in IGMP snooping–enabled VLANs.

Examples

# Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* | **all** } [**vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

group-address: Specifies an IGMP snooping group. The value range of *group-address* is 224.0.1.0 to 239.255.255.255.

all: Specifies all IGMP snooping groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset igmp-snooping group** to remove the dynamic group entries of a specific IGMP snooping group or all IGMP snooping groups.

This command works only in IGMP snooping–enabled VLANs.

This command cannot remove the static group entries of IGMP snooping groups.

Examples

# Remove the dynamic group entries of all IGMP snooping groups.

```
<Sysname> reset igmp-snooping group all
```

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset igmp-snooping statistics** to clear statistics for the IGMP messages learned through IGMP snooping.

Examples

# Clear statistics for the IGMP messages learned through IGMP snooping.

```
<Sysname> reset igmp-snooping statistics
```

router-aging-time (IGMP-snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1000.

Description

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 105 seconds.

This command works only in IGMP snooping–enabled VLANs.

Related commands: **igmp-snooping router-aging-time**.

Examples

# Set the aging timer for dynamic router ports to 100 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

source-deny (IGMP-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

IGMP-snooping view

Default level

2: System level

Parameters

interface-list: Specifies one or multiple ports. You can provide up to 10 port lists. For each list, you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

Description

Use **source-deny** to enable multicast source port filtering so that all multicast data packets are blocked.

Use **undo source-deny** to disable multicast source port filtering.

By default, multicast source port filtering is not enabled.

This command works in IGMP snooping–enabled VLANs.

Examples

# Enable source port filtering for multicast data on interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

PIM snooping configuration commands

display pim-snooping neighbor

Syntax

display pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping neighbor information of all VLANs.

slot *slot-number*: Displays the PIM snooping neighbor information of the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping neighbor** to display PIM snooping neighbor information.

Examples

# Display information about PIM snooping neighbors in VLAN 2.

```
<Sysname> display pim-snooping neighbor vlan 2
  Total number of neighbors: 2

  VLAN ID: 2
    Total number of neighbors: 2
    Neighbor        Port                     Expires   Option Flags
    10.1.1.2        GE1/0/1                   02:02:23  LAN Prune Delay(T)
    20.1.1.2        GE1/0/2                   03:00:05  LAN Prune Delay
```

Table 5 Command output

Field	Description
Total number of neighbors	Total number of PIM snooping neighbors.
Neighbor	IP address of the PIM snooping neighbor.
Port	Name of the port that connects to the PIM snooping neighbor.
Expires	Remaining time before the PIM snooping neighbor expires. *Never* means the PIM snooping neighbor never expires.
Option Flags	Possible values includes the following items: • **LAN Prune Delay**—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • **LAN Prune Delay(T)**—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled

display pim-snooping routing-table

Syntax

display pim-snooping routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping routing entries in all VLANs.

slot *slot-number*: Displays the PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping routing-table** to display the PIM snooping routing entries.

Examples

# Display the PIM snooping routing entries of VLAN 2.

```
<Sysname> display pim-snooping routing-table vlan 2 slot 1
  Total 1 entry(ies)
  FSM Flag: NI-no info, J-join, PP-prune pending

  VLAN ID: 2
    Total 2 entry(ies)
    (172.10.10.1, 225.1.1.1)
      Upstream neighbor: 20.1.1.1
        Upstream port: GE1/0/1
        Total number of downstream ports: 1
          1: GE1/0/3
             Expires: 00:03:01, FSM: J
      Upstream neighbor: 10.1.1.1
        Upstream port: GE1/0/2
        Total number of downstream ports: 1
          1: GE1/0/4
             Expires: 00:01:05, FSM: J
```

Table 6 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the PIM snooping routing table
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: • **NI**—Initial state • **J**—Join • **PP**—Prune pending
(172.10.10.1, 225.1.1.1)	(S, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
Upstream port	Upstream port of the (S, G) entry or (*, G) entry)
Expires	Expiration time of the downstream port
FSM	State machine flag of the downstream port

display pim-snooping statistics

Syntax

display pim-snooping statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping statistics** to display statistics for the PIM messages learned through PIM snooping.

Examples

# Display statistics for the PIM messages learned through PIM snooping.

```
<Sysname> display pim-snooping statistics
 Received PIMv2 hello: 100
 Received PIMv2 join/prune: 100
 Received PIMv2 error: 0
 Received PIMv2 messages in total: 200
 Received PIMv1 messages in total: 0
```

Table 7 Command output

Field	Description
Received PIMv2 hello	Number of received PIMv2 hello messages
Received PIMv2 join/prune	Number of received PIMv2 join/prune messages
Received PIMv2 error	Number of received PIMv2 messages with errors
Received PIMv2 messages in total	Total number of received PIMv2 messages
Received PIMv1 messages in total	Total number of received PIMv1 messages

pim-snooping enable

Syntax

pim-snooping enable

undo pim-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **pim-snooping enable** to enable PIM snooping in a VLAN.

Use **undo pim-snooping enable** to disable PIM snooping in a VLAN.

By default, PIM snooping is disabled.

Before you enable PIM snooping in a VLAN, be sure to enable IGMP snooping globally and specifically in the VLAN.

PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable**.

Examples

# Enable IGMP snooping globally, and enable IGMP snooping and PIM snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
```

reset pim-snooping statistics

Syntax

reset pim-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset pim-snooping statistics** to clear statistics for the PIM messages learned through PIM snooping.

Examples

# Clear statistics for the PIM messages learned through PIM snooping.

```
<Sysname> reset pim-snooping statistics
```

Multicast VLAN configuration commands

display multicast-vlan

Syntax

display multicast-vlan [*vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies a multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all multicast VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display multicast-vlan** to display information about the specified multicast VLAN.

Examples

# Display information about all multicast VLANs.

```
<Sysname> display multicast-vlan
 Total 2 multicast-vlan(s)

 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port

 Multicast vlan 200
   subvlan list:
    no subvlan
   port list:
    GE1/0/1                  GE1/0/2
```

Table 8 Command output

Field	Description
subvlan list	List of sub-VLANs of the multicast VLAN
port list	Port list of the multicast VLAN

multicast-vlan

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

View

System view

Default level

2: System level

Parameters

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

all: Specifies all multicast VLANs.

Description

Use **multicast-vlan** to configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.

Use **undo multicast-vlan** to remove the specified VLAN as a multicast VLAN.

The VLAN to be configured is not a multicast VLAN by default.

The specified VLAN to be configured as a multicast VLAN must exist.

The multicast VLAN feature cannot be enabled on a device with IP multicast routing enabled.

For a sub-VLAN-based multicast VLAN, you must enable IGMP snooping only in the multicast VLAN. For a port-based multicast VLAN, you must enable IGMP snooping in both the multicast VLAN and all the user VLANs.

Related commands: **igmp-snooping enable** and **multicast routing-enable**.

Examples

# Enable IGMP snooping in VLAN 100. Configure it as a multicast VLAN and enter multicast VLAN view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] igmp-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan 100
[Sysname-mvlan-100]
```

port (multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

View

Multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Specifies all the ports in the current multicast VLAN.

Description

Use **port** to assign the specified ports to the current multicast VLAN.

Use **undo port** to delete the specified ports or all ports from the current multicast VLAN.

By default, a multicast VLAN has no ports.

A port can belong to only one multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces as multicast VLAN ports.

Examples

# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

View

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

Default level

2: System level

Parameters

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

Description

Use **port multicast-vlan** to assign the current port to the specified multicast VLAN.

Use **undo port multicast-vlan** to restore the default.

By default, a port does not belong to any multicast VLAN.

A port can belong to only one multicast VLAN.

Examples

# Assign GigabitEthernet 1/0/1 to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan 100
```

subvlan (multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

View

Multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

all: Specifies all the sub-VLANs of the current multicast VLAN.

Description

Use **subvlan** to configure sub-VLANs for the current multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as sub-VLANs of the multicast VLAN must have existed and must not be multicast VLANs or sub-VLANs of another multicast VLAN.

The number of sub-VLANs of the multicast VLAN must not exceed the system-defined limit.

Examples

# Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] subvlan 10 to 15
```

MLD snooping configuration commands

display mld-snooping group

Syntax

display mld-snooping group [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the MLD snooping group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays MLD snooping group information in all VLANs.

slot *slot-number*: Displays information about MLD snooping multicast groups on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed MLD snooping group information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping group** to display MLD snooping group information, including both dynamic and static MLD snooping group entries.

Examples

# Display detailed MLD snooping group information in VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
        GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Attribute:    Host Port
      Host port(s):total 1 port(s).
        GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
    MAC group address:3333-0000-0101
      Host port(s):total 1 port(s).
        GE1/0/2
```

Table 9 Command output

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups
Total 1 IP Source(s).	Total number of IPv6 multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: **D**—Dynamic port **S**—Static port **C**—Port copied from a (*, G) entry to an (S, G) entry **P**—Port that IPv6 PIM snooping adds
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: **R**—Real egress sub-VLAN under the current entry, **C**—Sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port.
IP group address	Address of IPv6 multicast group
(::, FF1E::101)	(S, G) entry, double colon represents all the multicast sources
MAC group address	Address of MAC multicast group
Attribute	Attribute of IPv6 multicast group
Host port(s)	Number of member ports

display mld-snooping host

Syntax

display mld-snooping host vlan *vlan-id* **group** *ipv6-group-address* [**source** *ipv6-source-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by MLD snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *ipv6-group-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast group. The value of *ipv6-group-address* is in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast source.

slot *slot-number*: Displays information about the hosts tracked by MLD snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping host** to display information about the hosts tracked by MLD snooping.

Examples

# Display information about the hosts tracked by MLD snooping in multicast group FF1E::101 in VLAN 2.

```
<Sysname> display mld-snooping host vlan 2 group ff1e::101
VLAN(ID) : 2
  (::, FF1E::101)
    Port : GigabitEthernet1/0/1
      Host                                    Uptime          Expires
      1::1                                    00:02:20        00:00:40
      2::2                                    00:02:21        00:00:39
    Port : GigabitEthernet1/0/2
      Host                                    Uptime          Expires
      3::3                                    00:02:20        00:00:40
```

Table 10 Command output

Field	Description
(::, FF1E::101)	(S, G) entry, where :: indicates all IPv6 multicast sources.
Port	Member port

Field	Description
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where *timeout* means that the host has expired.

display mld-snooping statistics

Syntax

display mld-snooping statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping statistics** to display statistics for the MLD messages learned through MLD snooping.

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 error MLD messages:0.
```

Table 11 Command output

Field	Description
general queries	General query messages
specific queries	Multicast-address-specific query messages
reports	Report messages
dones	Done messages
reports with right and wrong records	Reports that contain correct and incorrect records
specific sg queries	Multicast-address-and-source-specific queries

dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

MLD-snooping view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **dot1p-priority** to set the 802.1p precedence for MLD messages globally.

Use **undo dot1p-priority** to restore the default.

The default 802.1p precedence for MLD messages is 0.

Examples

# Set the 802.1p precedence for MLD messages to 3 globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dot1p-priority 3
```

dscp (MLD-snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD-snooping view

Default level

2: System level

Parameters

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

Description

Use **dscp** to set the DSCP value for MLD messages.

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

The default DSCP value in MLD messages is 48.

Examples

# Set the DSCP value to 63 for MLD messages.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

fast-leave (MLD-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use **undo fast-leave** to disable fast-leave processing globally.

By default, fast-leave processing is disabled.

This command works in MLD snooping–enabled VLANs.

Related commands: **mld-snooping fast-leave**.

Examples

# Enable fast-leave processing globally in VLAN 2.

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

```
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

group-policy (MLD-snooping view)

Syntax

group-policy *acl6-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

MLD-snooping view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule matches the IPv6 multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **group-policy** to configure a global IPv6 multicast group filter, namely, to control the IPv6 multicast groups that a host can join.

Use **undo group-policy** to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally. Namely, any host can join any valid IPv6 multicast group.

If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **mld-snooping group-policy**.

Examples

# Apply ACL 2000 as an IPv6 multicast group filter so that hosts in VLAN 2 can join FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
 [Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

host-aging-time (MLD-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command works only in MLD snooping–enabled VLANs.

Related commands: **mld-snooping host-aging-time**.

Examples

# Set the aging timer for dynamic member ports to 300 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

host-tracking (MLD-snooping view)

Syntax

host-tracking

undo host-tracking

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the MLD snooping host tracking function globally.

Use **undo host-tracking** to disable the MLD snooping host tracking function globally.

By default, this function is disabled.

This command works only in MLD snooping–enabled VLANs.

Related commands: **display mld-snooping host** and **mld-snooping host-tracking**.

Examples

# Enable the MLD snooping host tracking function globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-tracking
```

last-listener-query-interval (MLD-snooping view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value range is 1 to 5.

Description

Use **last-listener-query-interval** to configure the MLD last-listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

By default, the MLD last-listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries.

This command works only in MLD snooping–enabled VLANs.

Related commands: **mld-snooping last-listener-query-interval**.

Examples

# Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

max-response-time (MLD-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

Use **max-response-time** to configure the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

By default, the maximum response delay for MLD general queries is 10 seconds.

This command works only in MLD snooping–enabled VLANs.

Related commands: **mld-snooping max-response-time** and **mld-snooping query-interval**.

Examples

# Set the maximum response delay for MLD general queries to 5 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

mld-snooping

Syntax

mld-snooping

undo mld-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping** to enable MLD snooping globally and enter MLD-snooping view.

Use **undo mld-snooping** to disable MLD snooping globally.

By default, MLD snooping is disabled.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping globally and enter MLD-snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

mld-snooping access-policy

Syntax

mld-snooping access-policy *acl6-number*

undo mld-snooping access-policy { *acl6-number* | **all** }

View

User profile view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IP packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX and TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

all: Specifies all IPv6 ACLs.

Description

Use **mld-snooping access-policy** to configure an IPv6 multicast user control policy.

Use **undo mld-snooping access-policy** to remove the configuration.

By default, no IPv6 user control policy is configured. Namely, a user can join any valid IPv6 multicast group.

You can use this command repeatedly to configure multiple IPv6 multicast user control policies.

Examples

# Create and enable a user profile named **abc**, and configure the user profile so that users in this user profile can join FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source ff03::101 16
[Sysname-acl6-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] mld-snooping access-policy 2001
[Sysname-user-profile-abc] quit
[Sysname] user-profile abc enable
```

mld-snooping done source-ip

Syntax

mld-snooping done source-ip { *ipv6-address* | **current-interface** }

undo mld-snooping done source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD done messages that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD done messages that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping done source-ip** to configure the source IPv6 address of the MLD done messages that the MLD snooping proxy sends.

Use **undo mld-snooping done source-ip** to restore the default.

By default, the source IPv6 address of the MLD done messages that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping done source-ip** command also applies when the simulated host sends MLD done messages.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD done messages that the MLD snooping proxy sends in VLAN 2 to FE80:0:0:1::1.

```
<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
```

mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority *priority-number*

undo mld-snooping dot1p-priority

View

VLAN view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **mld-snooping dot1p-priority** to set the 802.1p precedence for the MLD messages in a VLAN.

Use **undo mld-snooping dot1p-priority** to restore the default.

The default 802.1p precedence for the MLD messages in a VLAN is 0.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping in VLAN 2 and set the 802.1p precedence for the MLD messages in the VLAN 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
```

mld-snooping drop-unknown

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data for a VLAN.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data for a VLAN.

By default, this function is disabled, and unknown IPv6 multicast data is flooded in the VLAN.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **drop-unknown** and **mld-snooping enable**.

Examples

# Enable MLD snooping and the function for dropping unknown IPv6 multicast data in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

mld-snooping enable

Syntax

mld-snooping enable

undo mld-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **undo mld-snooping enable** to disable MLD snooping for a VLAN.

By default, MLD snooping is disabled in a VLAN.

MLD snooping must be enabled globally before it can be enabled in a VLAN

Related commands: **mld-snooping**.

Examples

# Enable MLD snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

mld-snooping fast-leave

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on the current port or group of ports.

By default, fast-leave processing is disabled.

This command works in MLD snooping–enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

# Enable fast-leave processing on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

mld-snooping general-query source-ip

Syntax

mld-snooping general-query source-ip { *ipv6-address* | **current-interface** }

undo mld-snooping general-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

current-interface: Sets the source IPv6 link-local address of MLD general queries to the IPv6 address of the current VLAN interface. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD general queries.

Description

Use **mld-snooping general-query source-ip** to configure the source IPv6 address of MLD general queries.

Use **undo mld-snooping general-query source-ip** to restore the default.

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

# In VLAN 2, enable MLD snooping and specify FE80:0:0:1::1 as the source IPv6 address of 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
```

mld-snooping group-limit

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

limit: Specifies the maximum number of IPv6 multicast groups that a port can join. The value ranges from 1 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping group-limit** to configure the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to restore the default.

By default, the upper limit is 1000.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **mld group-limit**.

Examples

# Configure to allow up to 10 IPv6 multicast groups that GigabitEthernet 1/0/1 in VLAN 2 can join.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Syntax

mld-snooping group-policy *acl6-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping group-policy** to configure an IPv6 multicast group filter on the current ports, namely, to control the multicast groups that the hosts on the port can join.

Use **undo mld-snooping group-policy** to remove the configured IPv6 multicast group filter on the current port or ports.

By default, no IPv6 multicast group filter is configured on a port. Namely, a host can join any valid IPv6 multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

# Apply ACL 2000 as an IPv6 multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

mld-snooping host-aging-time

Syntax

mld-snooping host-aging-time *interval*

undo mld-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

Use **mld-snooping host-aging-time** to set the aging timer for the dynamic member ports for a VLAN.

Use **undo mld-snooping host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **display mld-snooping host**, **host-aging-time** and **mld-snooping enable**.

Examples

# Enable MLD snooping and set the aging timer for dynamic member ports to 300 seconds in VLAN 2.

```
<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
```

mld-snooping host-join

Syntax

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

View

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

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the simulated host will join. The value ranges from FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the simulated host will join.

vlan *vlan-id*: Specifies a VLAN that comprises the port or ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping host-join** to enable simulated joining on a port. Namely, you configure a port as a simulated member host for the specified IPv6 multicast group or source and group.

Use **undo mld-snooping host-join** to remove the simulated member host from the specified IPv6 multicast group or source and group.

By default, this function is disabled.

This command works in MLD snooping–enabled VLANs. The version of MLD on the simulated member host is consistent with the version of MLD snooping that runs in the VLAN.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 to join (2002::22, FF3E::101) as a simulated host.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22 vlan
2
```

mld-snooping host-tracking

Syntax

mld-snooping host-tracking

undo mld-snooping host-tracking

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping host-tracking** to enable the MLD snooping host tracking function in a VLAN.

Use **undo mld-snooping host-tracking** to disable the MLD snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable MLD snooping for the VLAN first.

Related commands: **host-tracking**, and **mld-snooping enable**.

Examples

# Enable MLD snooping and the MLD snooping host tracking function for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-tracking
```

mld-snooping last-listener-query-interval

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value ranges from 1 to 5.

Description

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.

By default, the MLD last listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries in a VLAN.

You must enable MLD snooping for a VLAN before you configure this command for the VLAN.

Related commands: **last-listener-query-interval** and **mld-snooping enable**.

Examples

# Enable MLD snooping and set the MLD last listener query interval to 3 seconds in VLAN 2.

```
<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
```

mld-snooping max-response-time

Syntax

mld-snooping max-response-time *interval*

undo mld-snooping max-response-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

Use **mld-snooping max-response-time** to configure the maximum response delay for MLD general queries in the VLAN.

Use **undo mld-snooping max-response-time** to restore the default.

By default, the maximum response delay for MLD general queries is 10 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, and **mld-snooping query-interval**.

Examples

# Enable MLD snooping and set the maximum response delay for MLD general queries to 5 seconds in VLAN 2.

```
<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
```

mld-snooping overflow-replace

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement function on the current port.

Use **undo mld-snooping overflow-replace** to disable the IPv6 multicast group replacement function.

By default, the IPv6 multicast group replacement function is disabled.

This command works in MLD snooping–enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

# Enable the IPv6 multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

mld-snooping proxying enable

Syntax

mld-snooping proxying enable

undo mld-snooping proxying enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping proxying enable** to enable the MLD snooping proxying function in a VLAN.

Use **undo mld-snooping proxying enable** to disable the MLD snooping proxying function in a VLAN.

By default, MLD snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping and then MLD snooping proxying in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping proxying enable
```

mld-snooping querier

Syntax

mld-snooping querier

undo mld-snooping querier

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping querier** to enable the MLD snooping querier function.

Use **undo mld-snooping querier** to disable the MLD snooping querier function.

By default, the MLD snooping querier function is disabled.

This command takes effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

# Enable MLD snooping and the MLD snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

mld-snooping query-interval

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an MLD query interval in seconds, namely, the length of time that the device waits between sending MLD general queries. The value ranges from 2 to 300.

Description

Use **mld-snooping query-interval** to configure the MLD query interval.

Use **undo mld-snooping query-interval** to restore the default.

By default, the MLD query interval is 125 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, **mld-snooping max-response-time**, and **mld-snooping querier**.

Examples

# Enable MLD snooping and set the MLD query interval to 20 seconds in VLAN 2.

```
<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
```

mld-snooping report source-ip

Syntax

mld-snooping report source-ip { *ipv6-address* | **current-interface** }

undo mld-snooping report source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD reports that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD reports that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping report source-ip** to configure the source IPv6 address of the MLD reports that the MLD snooping proxy sends.

Use **undo mld-snooping report source-ip** to restore the default.

By default, the source IPv6 address of the MLD reports that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping report source-ip** command also applies when the simulated host sends MLD reports.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD reports that the MLD snooping proxy sends in VLAN 2 to FE80:0:0:1::1.

```
<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
```

mld-snooping router-aging-time

Syntax

mld-snooping router-aging-time *interval*

undo mld-snooping router-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports, in seconds. The value ranges from 1 to 1,000.

Description

Use **mld-snooping router-aging-time** to set the aging timer for the dynamic router ports for a VLAN.

Use **undo mld-snooping router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable** and **router-aging-time**.

Examples

# Enable MLD snooping and set the aging timer for the dynamic router ports to 100 seconds in VLAN 2.

```
<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
```

mld-snooping router-port-deny

Syntax

mld-snooping router-port-deny [**vlan** *vlan-list*]

undo mld-snooping router-port-deny [**vlan** *vlan-list*]

View

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

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo mld-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

This command works in MLD snooping–enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified 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 source-deny

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

This command works in MLD snooping–enabled VLANs.

Examples

# Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping source-deny
```

mld-snooping special-query source-ip

Syntax

mld-snooping special-query source-ip { *ipv6-address* | **current-interface** }

undo mld-snooping special-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

current-interface: Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD multicast-address-specific queries.

Description

Use **mld-snooping special-query source-ip** to configure the source IPv6 address of MLD multicast-address-specific queries.

Use **undo mld-snooping special-query source-ip** to restore the default.

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

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
```

mld-snooping static-group

Syntax

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

View

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

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the port will join as a static member port. The value ranges from FFxy::/16—excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the port will join as a static member port.

vlan *vlan-id*: Specifies the VLAN that comprises the Ethernet ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping static-group** to configure the static IPv6 (*, G) or (S, G) joining function, that is, to configure the port as a static member port of an IPv6 multicast group or source and group.

Use **undo mld-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 as a static member port for (2002::22, FF3E::101).

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 source-ip 2002::22
vlan 2
```

mld-snooping static-router-port

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port vlan *vlan-id*

View

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

Default level

2: System level

Parameters

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

Description

Use **mld-snooping static-router-port** to configure the current port as a static router port.

Use **undo mld-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

This command works in MLD snooping–enabled VLANs.

This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan**.

Examples

# Enable the static router port function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2
```

mld-snooping version

Syntax

mld-snooping version *version-number*

undo mld-snooping version

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an MLD snooping version. The value can be 1 or 2.

Description

Use **mld-snooping version** to configure the MLD snooping version.

Use **undo mld-snooping version** to restore the default.

By default, the MLDv1 snooping is used.

This command can take effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

# Enable MLD snooping in VLAN 2, and specify MLDv2 snooping.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

overflow-replace (MLD-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **overflow-replace** to enable the IPv6 multicast group replacement function globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement function globally.

By default, the IPv6 multicast group replacement function is disabled globally.

This command works in MLD snooping–enabled VLANs.

Related commands: **mld-snooping overflow-replace**.

Examples

# Enable the IPv6 multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

report-aggregation (MLD-snooping view)

Syntax

report-aggregation

undo report-aggregation

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

Use **report-aggregation** to enable MLD report suppression.

Use **undo report-aggregation** to disable MLD report suppression.

By default, MLD report suppression is enabled.

This command works in MLD snooping–enabled VLANs.

Examples

# Disable MLD report suppression.

```
<Sysname> system-view
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] undo report-aggregation
```

reset mld-snooping group

Syntax

reset mld-snooping group { *ipv6-group-address* | **all** } [**vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group. The value range of *ipv6-group-address* is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset mld-snooping group** to remove the dynamic group entries of a specified MLD snooping group or all MLD snooping groups.

This command works only in MLD snooping–enabled VLANs.

This command cannot remove the static group entries of MLD snooping groups.

Examples

# Remove the dynamic group entries of all MLD snooping groups.

```
<Sysname> reset mld-snooping group all
```

reset mld-snooping statistics

Syntax

reset mld-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset mld-snooping statistics** to clear statistics for the MLD messages learned through MLD snooping.

Examples

# Clear statistics for the MLD messages learned through MLD snooping.

```
<Sysname> reset mld-snooping statistics
```

router-aging-time (MLD-snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1,000.

Description

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

By default, the aging time of a dynamic router port is 260 seconds.

This command works only in MLD snooping–enabled VLANs.

Related commands: **mld-snooping router-aging-time**.

Examples

# Set the aging timer for dynamic router ports to 100 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

source-deny (MLD-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

MLD-snooping view

Default level

2: System level

Parameters

interface-list: Specifies a list of ports. You can specify multiple ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }, where *interface-type* is the port type and *interface-number* is the port number.

Description

Use **source-deny** to enable IPv6 multicast source port filtering, namely, to filter out all the received IPv6 multicast packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

This command works in MLD snooping–enabled VLANs.

Examples

# Enable source port filtering for IPv6 multicast data on interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

IPv6 PIM snooping configuration commands

display pim-snooping ipv6 neighbor

Syntax

display pim-snooping ipv6 neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the IPv6 PIM snooping neighbor information in all VLANs.

slot *slot-number*: Displays the IPv6 PIM snooping neighbor information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping ipv6 neighbor** to display IPv6 PIM snooping neighbor information.

Examples

# Display the IPv6 PIM snooping neighbor information of VLAN 2.

```
<Sysname> display pim-snooping ipv6 neighbor vlan 2
  Total number of neighbors: 2

  VLAN ID: 2
    Total number of neighbors: 2
    Neighbor         Port                     Expires   Option Flags
    FE80::6401:101   GE1/0/1                   02:02:23  LAN Prune Delay(T)
    FE80::C801:101   GE1/0/2                   03:00:05  LAN Prune Delay
```

Table 12 Command output

Field	Description
Total number of neighbors	Total number of IPv6 PIM snooping neighbors.
Neighbor	IP address of the IPv6 PIM snooping neighbor.
Port	Name of the port that connects to the IPv6 PIM snooping neighbor.
Expires	Remaining time before the IPv6 PIM snooping neighbor expires. *Never* means the IPv6 PIM snooping neighbor never expires.
Option Flags	Possible values includes the following items: • **LAN Prune Delay**—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • **LAN Prune Delay(T)**—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled

display pim-snooping ipv6 routing-table

Syntax

display pim-snooping ipv6 routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the IPv6 PIM snooping routing entries in all VLANs.

slot *slot-number*: Displays the IPv6 PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping ipv6 routing-table** to display the IPv6 PIM snooping routing table.

Examples

# Display the IPv6 PIM snooping routing entries of VLAN 2.

```
<Sysname> display pim-snooping ipv6 routing-table vlan 2 slot 1
  Total 1 entry(ies)
  FSM Flag: NI-no info, J-join, PP-prune pending

  VLAN ID: 2
    Total 2 entry(ies)
    (2000::1, FF1E::1)
      Upstream neighbor: FE80::101
        Upstream port: GE1/0/1
        Total number of downstream ports: 2
          1: GE1/0/3
             Expires: 00:03:01, FSM: J
      Upstream neighbor: FE80::102
        Upstream port: GE1/0/2
        Total number of downstream ports: 1
          1: GE1/0/4
             Expires: 00:01:05, FSM: J
```

Table 13 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the IPv6 PIM snooping routing table
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: • **NI**—Initial state • **J**—Join • **PP**—Prune pending
(2000::1, FF1E::1)	(S, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
Upstream port	Upstream port of the (S, G) entry or (*, G) entry)
Expires	Expiration time of the downstream port
FSM	State machine of the downstream port

display pim-snooping ipv6 statistics

Syntax

display pim-snooping ipv6 statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pim-snooping ipv6 statistics** to display statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

Examples

# Display statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

```
<Sysname> display pim-snooping ipv6 statistics
 Received IPv6 PIM IPv6 hello: 100
 Received IPv6 PIM IPv6 join/prune: 100
 Received IPv6 PIM IPv6 error: 0
 Received IPv6 PIM IPv6 messages in total: 200
```

Table 14 Command output

Field	Description
Received IPv6 PIM IPv6 hello	Number of received IPv6 PIM hello messages
Received IPv6 PIM IPv6 join/prune	Number of received IPv6 PIM join/prune messages
Received IPv6 PIM IPv6 error	Number of received IPv6 PIM messages with errors
Received IPv6 PIM IPv6 messages in total	Total number of received IPv6 PIM messages

pim-snooping ipv6 enable

Syntax

pim-snooping ipv6 enable

undo pim-snooping ipv6 enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **pim-snooping ipv6 enable** to enable IPv6 PIM snooping in a VLAN.

Use **undo pim-snooping ipv6 enable** to disable IPv6 PIM snooping in a VLAN.

By default, IPv6 PIM snooping is disabled.

Before you enable IPv6 PIM snooping in a VLAN, be sure to enable MLD snooping globally and specially in the VLAN.

IPv6 PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **mld-snooping enable**.

Examples

# Enable MLD snooping globally, and enable MLD snooping and IPv6 PIM snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] pim-snooping ipv6 enable
```

reset pim-snooping ipv6 statistics

Syntax

reset pim-snooping ipv6 statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset pim-snooping ipv6 statistics** to clear statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

Examples

# Clear statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

```
<Sysname> reset pim-snooping ipv6 statistics
```

IPv6 multicast VLAN configuration commands

display multicast-vlan ipv6

Syntax

display multicast-vlan ipv6 [*vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies an IPv6 multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all IPv6 multicast VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

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

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display multicast-vlan ipv6** to display information about the specified IPv6 multicast VLAN or all IPv6 multicast VLANs.

Examples

# Display information about all IPv6 multicast VLANs.

```
<Sysname> display multicast-vlan ipv6
 Total 2 IPv6 multicast-vlan(s)
 IPv6 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port
 IPv6 Multicast vlan 200
   subvlan list:
    no subvlan
   port list:
    GE1/0/1                 GE1/0/2
```

Table 15 Command output

Field	Description
subvlan list	List of sub-VLANs of the IPv6 multicast VLAN
port list	Port list of the IPv6 multicast VLAN

multicast-vlan ipv6

Syntax

multicast-vlan ipv6 *vlan-id*

undo multicast-vlan ipv6 { **all** | *vlan-id* }

View

System view

Default level

2: System level

Parameters

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

all: Specifies all IPv6 multicast VLANs.

Description

Use **multicast-vlan ipv6** to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use **undo multicast-vlan ipv6** to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

The specified VLAN to be configured as an IPv6 multicast VLAN must exist.

The IPv6 multicast VLAN feature cannot be enabled on a device with IPv6 multicast routing enabled.

For a sub-VLAN-based IPv6 multicast VLAN, you must enable MLD snooping only in the IPv6 multicast VLAN. For a port-based IPv6 multicast VLAN, you must enable MLD snooping in both the IPv6 multicast VLAN and all the user VLANs.

Related commands: **mld-snooping enable** and **multicast ipv6 routing-enable**.

Examples

# Enable MLD snooping in VLAN 100. Configure it as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100]
```

port (IPv6 multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Specifies all the ports in the current IPv6 multicast VLAN.

Description

Use **port** to assign the specified ports to the current IPv6 multicast VLAN.

Use **undo port** to delete the specified ports from the current IPv6 multicast VLAN.

By default, an IPv6 multicast VLAN has no ports.

A port can belong to only one IPv6 multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces to a multicast VLAN.

Examples

# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan ipv6

Syntax

port multicast-vlan ipv6 *vlan-id*

undo port multicast-vlan ipv6

View

Ethernet interface view, Layer 2 aggregate interface view, port group view.

Default level

2: System level

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its ID, in the range of 1 to 4094.

Description

Use **port multicast-vlan ipv6** to assign the current port to the specified IPv6 multicast VLAN.

Use **undo port multicast-vlan ipv6** to restore the default.

By default, a port does not belong to any IPv6 multicast VLAN.

A port can belong to only one IPv6 multicast VLAN.

Examples

# Assign GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan ipv6 100
```

subvlan (IPv6 multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

all: Specifies all the sub-VLANs of the current IPv6 multicast VLAN.

Description

Use **subvlan** to configure sub-VLANs for the current IPv6 multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of any other IPv6 multicast VLAN.

The number of sub-VLANs of the IPv6 multicast VLAN must not exceed the system-defined limit.

Examples

# Configure VLAN 10 through VLAN 15 as sub-VLANs of IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

Index

Contents

ACL configuration commands

acl

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl { **all** | **name** *acl-name* | **number** *acl-number* }

View

System view

Default level

2: System level

Parameters

number *acl-number*: Specifies the number of an access control list (ACL):

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *acl-name*: Assigns a name to the ACL for easy identification. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter, and to avoid confusion, cannot be **all**.

match-order: Sets the order in which ACL rules are compared against packets:

- **auto**—Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. For more information, see *ACL and QoS Configuration Guide*.
- **config**—Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

all: Deletes all IPv4 ACLs and Ethernet frame header ACLs.

Description

Use **acl** to create an IPv4 ACL or an Ethernet frame header ACL, and enter its view. If the ACL has been created, you enter its view directly.

Use **undo acl** to delete the specified IPv4 or Ethernet frame header ACL, or all IPv4 and Ethernet frame header ACLs.

By default, no ACL exists.

You can assign a name to an IPv4 or Ethernet frame header ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

You can change match order only for ACLs that do not contain any rules.

To display any ACLs you have created, use the **display acl** command.

Examples

# Create IPv4 basic ACL 2000, and enter its view.

```
<Sysname> system-view
```

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

# Create IPv4 basic ACL 2001 with the name **flow**, and enter its view.

```
<Sysname> system-view
[Sysname] acl number 2001 name flow
[Sysname-acl-basic-2001-flow]
```

acl copy

Syntax

acl copy { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

Default level

2: System level

Parameters

source-acl-number: Specifies an existing source ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument takes a case-insensitive string of 1 to 63 characters.

dest-acl-number: Assigns a unique number to the ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *dest-acl-name*: Assigns a unique name to the ACL you are creating. The *dest-acl-name* takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

Description

Use **acl copy** to create an IPv4 or an Ethernet frame header ACL by copying an ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

You can assign a name for an ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

Examples

# Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

acl ipv6

Syntax

acl ipv6 number *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

View

System view

Default level

2: System level

Parameters

number *acl6-number*: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *acl6-name*: Assigns a name to the IPv6 ACL for easy identification. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter, and to avoid confusion, cannot be **all**.

match-order: Sets the order in which ACL rules are compared against packets:

- **auto**—Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. For more information, see *ACL and QoS Configuration Guide*.
- **config**—Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

all: Delete all IPv6 ACLs.

Description

Use **acl ipv6** to create an IPv6 ACL and enter its ACL view. If the ACL has been created, you enter its view directly.

Use **undo acl ipv6** to delete the specified IPv6 ACL or all IPv6 ACLs.

By default, no ACL exists.

You can assign a name to an IPv6 ACL only when you create it. After an IPv6 ACL is created, you cannot rename it or remove its name.

You can change match order only for ACLs that do not contain any rules.

To display any ACLs you have created, use the **display acl ipv6** command.

Examples

# Create IPv6 ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

# Create IPv6 basic ACL 2001 with the name **flow**, and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001 name flow
[Sysname-acl6-basic-2001-flow]
```

acl ipv6 copy

Syntax

acl ipv6 copy { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

View

System view

Default level

2: System level

Parameters

source-acl6-number: Specifies an existing source IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *source-acl6-name*: Specifies an existing source IPv6 ACL by its name. The *source-acl6-name* argument takes a case-insensitive string of 1 to 63 characters.

dest-acl6-number: Assigns a unique number to the IPv6 ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *dest-acl6-name*: Assigns a unique name to the IPv6 ACL you are creating. The *dest-acl6-name* takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

Description

Use **acl ipv6 copy** to create an IPv6 ACL by copying an IPv6 ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

You can assign a name to an IPv6 ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

Examples

# Create IPv6 basic ACL 2002 by copying IPv6 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2001 to 2002
```

acl ipv6 logging frequence

Syntax

acl ipv6 logging frequence *frequence*

undo acl ipv6 logging frequence

View

System view

Default level

2: System level

Parameters

frequence: Specifies the interval in minutes at which IPv6 packet filtering logs are generated and output. It must be a multiple of 5, in the range of 0 to 1440. To disable generating IPv6 logs, assign 0 to the argument.

Description

Use **acl ipv6 logging frequence** to set the interval for generating and outputting IPv6 packet filtering logs. The log information includes the number of matching IPv6 packets and the matching IPv6 ACL rules. This command logs only for IPv6 basic and advanced ACL rules that have the **logging** keyword.

Use **undo acl ipv6 logging frequence** to restore the default.

By default, the interval is 0. No IPv6 packet filtering logs are generated.

Related commands: **packet-filter ipv6**, **rule (IPv6 advanced ACL view)**, and **rule (IPv6 basic ACL view)**.

Examples

# Enable the device to generate and output IPv6 packet filtering logs at 10-minute intervals.

```
<Sysname> system-view
[Sysname] acl ipv6 logging frequence 10
```

acl ipv6 name

Syntax

acl ipv6 name *acl6-name*

View

System view

Default level

2: System level

Parameters

acl6-name: Specifies the name of an existing IPv6 ACL, a case-insensitive string of 1 to 63 characters. It must start with an English letter.

Description

Use **acl ipv6 name** to enter the view of an IPv6 ACL that has a name.

Related commands: **acl ipv6**.

Examples

# Enter the view of IPv6 ACL **flow**.

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

acl logging frequence

Syntax

acl logging frequence *frequence*

undo acl logging frequence

View

System view

Default level

2: System level

Parameters

frequence: Specifies the interval in minutes at which IPv4 packet filtering logs are generated and output. It must be a multiple of 5, in the range of 0 to 1440. To disable generating IPv4 logs, assign 0 to the argument.

Description

Use **acl logging frequence** to set the interval for generating and outputting IPv4 packet filtering logs. The log information includes the number of matching IPv4 packets and the matching IPv4 ACL rules. This command logs only for IPv4 basic and advanced ACL rules that have the **logging** keyword.

Use **undo acl logging frequence** to restore the default.

By default, the interval is 0. No IPv4 packet filtering logs are generated.

Related commands: **packet-filter**, **rule (IPv4 advanced ACL view)**, and **rule (IPv4 basic ACL view)**.

Examples

# Enable the device to generate and output IPv4 packet filtering logs at 10-minute intervals.

```
<Sysname> system-view
[Sysname] acl logging frequence 10
```

acl name

Syntax

acl name *acl-name*

View

System view

Default level

2: System level

Parameters

acl-name: Specifies the IPv4 ACL name, a case-insensitive string of 1 to 63 characters. It must start with an English letter. The IPv4 ACL must already exist.

Description

Use **acl name** to enter the view of an IPv4 ACL that has a name.

Related commands: **acl**.

Examples

# Enter the view of IPv4 ACL **flow**.

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2001-flow]
```

description

Syntax

description *text*

undo description

View

IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default level

2: System level

Parameters

text: ACL description, a case-sensitive string of 1 to 127 characters.

Description

Use **description** to configure a description for an ACL.

Use **undo description** to remove the ACL description.

By default, an ACL has no ACL description.

Related commands: **display acl** and **display acl ipv6**.

Examples

# Configure a description for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This is an IPv4 basic ACL.
```

# Configure a description for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

display acl

Syntax

display acl { *acl-number* | **all** | **name** *acl-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Displays information for all IPv4 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

slot *slot-number*: Displays match statistics for ACLs on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays matches statistics for ACLs on all member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display acl** to display configuration and match statistics for the specified or all IPv4 ACLs.

This command displays ACL rules in config or depth-first order, whichever is configured.

Examples

# Display the configuration and match statistics for all IPv4 ACLs.

```
<Sysname> display acl all
Basic ACL  2000, named flow, 2 rules,
Statistics is enabled
ACL's step is 5
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (5 times matched)

Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 10 permit source 1.1.1.1 0
 rule 10 comment This rule is used in rd.
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

Table 1 Command output

Field	Description
Basic ACL 2000	Category and number of the ACL. The following field information is about IPv4 basic ACL 2000.

Field	Description
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
2 rules	The ACL contains two rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
Statistics is enabled	The rule match counting is enabled for this ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
5 times matched	There have been five matches for the rule. If the **counting** keyword is configured for the rule or the **hardw**are-count enable command is enabled for the ACL, the statistic counts both rule matches performed in both software and hardware. Otherwise, the statistics counts only rule matches performed in software.
rule 10 comment This rule is used in rd.	The description of ACL rule 10 is "This rule is used in rd."

display acl ipv6

Syntax

display acl ipv6 { *acl6-number* \| **all** \| **name** *acl6-name* } [**slot** *slot-number*] [**|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

all: Displays information for all IPv6 ACLs.

name *acl6-name*: Specifies an IPv6 ACL by its name. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

slot *slot-number*: Displays the match statistics for IPv6 ACLs on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays match statistics for IPv6 ACLs on all member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display acl ipv6** to display the configuration and match statistics for the specified IPv6 ACL or all IPv6 ACLs.

This command displays ACL rules in config or depth-first order, whichever is configured.

Examples

# Display the configuration and match statistics for all IPv6 ACLs.

```
<Sysname> display acl ipv6 all
 Basic IPv6 ACL  2000, named flow, 2 rules,
 Statistics is enabled
 ACL's step is 5
 rule 0 permit
 rule 5 permit source 1::/64 (5 times matched)

 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit source1::/64
 rule 10 comment This rule is used in rd.
 rule 5 permit source 2::/64
 rule 0 permit
```

Table 2 Command output

Field	Description
Basic IPv6 ACL 2000	Category and number of the ACL. The following field information is about this IPv6 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
2 rules	The ACL contains two rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
Statistics is enabled	The rule match counting is enabled for this ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
5 times matched	There have been five matches for the rule. If the **counting** keyword is configured for the rule or the **hardware-count enable** command is enabled for the ACL, the statistic counts both rule matches performed in both software and hardware. Otherwise, the statistics counts only rule matches performed in software.
rule 10 comment This rule is used in rd.	The description of ACL rule 10 is "This rule is used in rd."

display acl resource

Syntax

display acl resource [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the usage of ACL rules on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays the usage of ACL rules on all member switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display acl resource** to display the usage of ACL rules.

Examples

# Display the usage of ACL rules on a device.

```
<Sysname> display acl resource
Interface:
   GE1/0/1 to GE1/0/24
---------------------------------------------------------------------
 Type           Total       Reserved    Configured  Remaining    Usage
---------------------------------------------------------------------
 IFP ACL        2048        768         3           1277         37%
 IFP Meter      1024        384         0           640          37%
 IFP Counter    1024        384         3           637          37%

 Interface:
   GE1/0/25 to GE1/0/52
---------------------------------------------------------------------
 Type           Total       Reserved    Configured  Remaining    Usage
---------------------------------------------------------------------
 IFP ACL        2048        768         0           1280         37%
 IFP Meter      1024        384         0           640          37%
 IFP Counter    1024        384         0           640          37%
```

Table 3 Command output

Field	Description
Interface	Interface indicated by its type and number
Type	Rule type: - **IFP ACL**—ACL rules applied to inbound traffic - **IFP Meter**—Traffic policing rules for inbound traffic - **IFP Counter**—Traffic counting rules for inbound traffic
Total	Total number of ACL rules supported
Reserved	Number of reserved ACL rules
Configured	Number of ACL rules that have been applied
Remaining	Number of ACL rules that you can apply
Usage	Usage of the ACL rules

display packet-filter

Syntax

display packet-filter { { **all** | **interface** *interface-type interface-number* } [**inbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound**] [**slot** *slot-number*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Specifies all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number. VLAN interfaces are not supported.

inbound: Specifies the inbound direction.

interface vlan-interface *vlan-interface-number*: Specifies a VLAN interface by its number.

slot *slot-number*: Specifies an IRF member switch. The *slot-number* argument is the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays application status of incoming and outgoing packet filtering ACLs for VLAN interfaces of the master.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display packet-filter** to display whether an ACL has been successfully applied to an interface for packet filtering.

The ACL application status may be different on the master and on an IRF member switch because of ACL resource insufficiency. You can specify the slot number in the **display packet-filter** command to check the ACL application status on the member switch.

Examples

# Display the application status of packet filtering ACLs for interface GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 2001, Successful
```

Table 4 Command output

Field	Description
Interface	Interface to which the ACL applies.
In-bound Policy	ACL used for filtering incoming traffic on the interface.
acl 2001, Successful	IPv4 ACL 2001 has been applied to the interface.

display time-range

Syntax

display time-range { *time-range-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

time-range-name: Specifies a time range name, a case-insensitive string of 1 to 32 characters. It must start with an English letter.

all: Displays the configuration and status of all existing time ranges.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display time-range** to display the configuration and status of the specified time range or all time ranges.

Examples

# Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 4/13/2010 Tuesday

Time-range : t4 ( Inactive )
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2010 to 23:59 1/31/2010
 from 00:00 6/1/2010 to 23:59 6/30/2010
```

Table 5 Command output

Field	Description
Current time	Current system time
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time

hardware-count enable

Syntax

hardware-count enable

undo hardware-count enable

View

IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default level

2: System level

Parameters

None

Description

Use **hardware-count enable** to enable counting ACL rule matches performed in hardware. The device automatically counts the rule match counting performed in software.

Use **undo hardware-count enable** to disable counting ACL rule matches performed in hardware. This command also resets the hardware match counters for all rules in the ACL. For a rule configured with the **counting** keyword, this command only resets the rule's hardware match counter.

By default, ACL rule matches performed in hardware are not counted.

The **hardware-count enable** command enables match counting for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules. For an individual rule, rule match counting works as long as either the **hardware-count enable** command or the **counting** keyword is configured.

When an ACL is referenced by a QoS policy, this command or the **counting** keyword does not take effect. No ACL rule matches are counted.

Related commands: **display acl**, **display acl ipv6**, and **rule**.

Examples

# Enable rule match counting for IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] hardware-count enable
```

# Enable rule match counting for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] hardware-count enable
```

packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } **inbound**

undo packet-filter { *acl-number* | **name** *acl-name* } **inbound**

View

Layer 2 Ethernet interface view, VLAN interface view

Default level

2: System level

Parameters

acl-number: Specifies an IPv4 ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *acl-name*: Specifies an IPv4 ACL by its name. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

inbound: Filters incoming packets.

Description

Use **packet-filter** to apply an IPv4 basic, IPv4 advanced, or Ethernet frame header ACL to an interface to filter packets.

Use **undo packet-filter** to restore the default.

By default, an interface does not filter packets.

Related commands: **display packet-filter**.

Examples

# Apply IPv4 ACL 2001 to filter incoming traffic on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

packet-filter ipv6

Syntax

packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } **inbound**

undo packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } **inbound**

View

Layer 2 Ethernet interface view, VLAN interface view

Default level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *acl6-name*: Specifies an IPv6 ACL by its name. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

inbound: Filters incoming IPv6 packets

Description

Use **packet-filter ipv6** to apply an IPv6 basic or IPv6 advanced ACL to an interface to filter IPv6 packets.

Use **undo packet-filter ipv6** to restore the default.

By default, an interface does not filter IPv6 packets.

Related commands: **display packet-filter**.

Examples

# Apply IPv6 ACL 2500 to filter incoming packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2500 inbound
```

reset acl counter

Syntax

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

View

User view

Default level

2: System level

Parameters

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs

- 4000 to 4999 for Ethernet frame header ACLs

all: Clears statistics for all IPv4 and Ethernet frame header ACLs.

name *acl-name*: Specifies an IPv4 or Ethernet frame header ACL by its name. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

Description

Use **reset acl counter** to clear statistics for the specified IPv4 or Ethernet frame header ACL, or all IPv4 and Ethernet frame header ACLs.

Related commands: **display acl**.

Examples

# Clear statistics for IPv4 basic ACL 2001.

```
<Sysname> reset acl counter 2001
```

# Clear statistics for IPv4 ACL **flow**.

```
<Sysname> reset acl counter name flow
```

reset acl ipv6 counter

Syntax

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

View

User view

Default level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

all: Clears statistics for all IPv6 basic and advanced ACLs.

name *acl6-name*: Specifies an IPv6 ACL by its name. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

Description

Use **reset acl ipv6 counter** to clear statistics for the specified IPv6 ACL or all IPv6 basic and IPv6 advanced ACLs.

Related commands: **display acl ipv6**.

Examples

# Clear statistics for IPv6 basic ACL 2001.

```
<Sysname> reset acl ipv6 counter 2001
```

# Clear statistics for IPv6 ACL **flow**.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (Ethernet frame header ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-addr dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

View

Ethernet frame header ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

cos *vlan-pri:* Matches an 802.1p priority. The *vlan-pri* argument can be a number in the range of 0 to 7, or in words, **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Counts the number of times the Ethernet frame header ACL rule has been matched in hardware.

dest-mac *dest-addr dest-mask:* Matches a destination MAC address range. The *dest-addr* and *dest-mask* arguments represent a destination MAC address and mask in H-H-H format.

lsap *lsap-type lsap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a 16-bit hexadecimal number that represents the encapsulation format. The *lsap-type-mask* argument is a 16-bit hexadecimal number that represents the LSAP mask.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Ethernet frame header. The *protocol-type* argument is a 16-bit hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The *protocol-type-mask* argument is a 16-bit hexadecimal number that represents a protocol type mask.

source-mac *sour-addr source-mask:* Matches a source MAC address range. The *sour-addr* argument represents a source MAC address, and the *sour-mask* argument represents a mask in H-H-H format.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule; however, the rule using the time range can take effect only after you configure the timer range.

Description

Use **rule** to create or edit an Ethernet frame header ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an Ethernet frame header ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

By default, an Ethernet frame header ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

Related commands: **acl**, **display acl**, **step**, and **time-range**.

NOTE:

If the Ethernet frame header ACL is for QoS traffic classification or packet filtering, to use the **lsap** keyword, the *lsap-type* argument must be AAAA, and the *lasp-type-mask* argument must be FFFF. Otherwise, the ACL cannot be function normally.

Examples

# Create a rule in ACL 4000 to permit ARP packets and deny RARP packets.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule permit type 0806 ffff
[Sysname-acl-ethernetframe-4000] rule deny type 8035 ffff
```

rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **precedence** *precedence* | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos*] *

undo rule rule-id [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **fragment** | **icmp-type** | **logging** | **precedence** | **source** | **source-port** | **time-range** | **tos**] *

View

IPv4 advanced ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Protocol carried by IPv4. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). Table 6 describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

Table 6 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address	The *sour-addr sour-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword specifies any source IP address.
destination { *dest-addr dest-wildcard* | **any** }	Specifies a destination address	The *dest-addr dest-wildcard* arguments represent a destination IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword represents any destination IP address.
counting	Counts the number of times the IPv4 ACL rule has been matched in hardware.	—
precedence *precedence*	Specifies an IP precedence value	The *precedence* argument can be a number in the range of 0 to 7, or in words, **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference	The *tos* argument can be a number in the range of 0 to 15, or in words, **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
logging	Logs matching packets	This function requires that the module (for example, packet filter) that uses the ACL supports logging.
fragment	Applies the rule to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.

Parameters	Function	Description
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule; however, the rule using the time range can take effect only after you configure the timer range.

NOTE:

If you provide the **precedence** or **tos** keyword in addition to the **dscp** keyword, only the **dscp** keyword takes effect.

If the *protocol* argument takes **tcp** (6) or **udp** (7), you can set the parameters shown in Table 7.

Table 7 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented in these words: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in one rule are ANDed.

Parameters	Function	Description
established	Specifies the flags for indicating the established status of a TCP connection	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument takes **icmp** (1), you can set the parameters shown in Table 8.

Table 8 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* [*icmp-code*] | *icmp-message* }	Specifies the ICMP message type and code	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 9.

Table 9 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0

ICMP message name	ICMP message type	ICMP message code
ttl-exceeded	11	0

Description

Use **rule** to create or edit an IPv4 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

By default, an IPv4 advanced ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

If an IPv4 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify **neq** for the *operator* argument.
- The **logging** and **counting** keywords (even if specified) do not take effect for QoS traffic classification.

Related commands: **acl**, **display acl**, **step**, and **time-range**.

Examples

# Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24, and enable logging matching packets.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80 logging
```

# Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit ip
[Sysname-acl-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
```

# Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl number 3002
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp-data
```

# Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl number 3003
[Sysname-acl-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-adv-3003] rule permit udp source-port eq snmptrap
```

```
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmptrap
```

rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range**] *

View

IPv4 basic ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv4 ACL rule has been matched in hardware.

fragment: Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

logging: Logs matching packets. This function is available only when the application module (such as the packet filter) that uses the ACL supports the logging function.

source { *sour-addr sour-wildcard* | **any** }: Matches a source address. The *sour-addr sour-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. A wildcard mask of zeros specifies a host address. The **any** keyword represents any source IP address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule; however, the rule using the time range can take effect only after you configure the timer range.

Description

Use **rule** to create or edit an IPv4 basic ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

By default, an IPv4 basic ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

Related commands: **acl**, **display acl**, **step**, and **time-range**.

NOTE:

If an IPv4 basic ACL is for QoS traffic classification, the **logging** and **counting** keywords (even if specified) do not take effect.

Examples

# Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP segment but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] rule deny source any
```

rule (IPv6 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source source-prefix* | *source/source-prefix* **|** **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **source** | **source-port** | **time-range**] *

View

IPv6 advanced ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Matches protocol carried over IPv6. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). Table 10 describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

Table 10 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address	The *source* and *source-prefix* arguments represent an IPv6 source address, and prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address	The *dest* and *dest-prefix* arguments represent a destination IPv6 address, and prefix length in the range of 1 to 128. The **any** keyword specifies any IPv6 destination address.
counting	Counts the number of times the IPv6 ACL rule has been matched in hardware	—
dscp *dscp*	Specifies a DSCP preference	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header	The *flow-label-value* argument is in the range of 0 to 1048575.
logging	Logs matching packets	This function requires that the module (for example, packet filter) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies the type of routing header	The *routing-type* argument takes a value in the range of 0 to 255. If no routing type header is specified, the rule applies to the IPv6 packets that have any type of routing header.
fragment	Applies the rule to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule; however, the rule using the time range can take effect only after you configure the timer range.

If the *protocol* argument takes **tcp** (6) or **udp** (17), you can set the parameters shown in Table 11.

Table 11 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented in these words: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in one rule are ANDed.
established	Specifies the flags for indicating the established status of a TCP connection	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument takes **icmpv6** (58), you can set the parameters shown in Table 12.

Table 12 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 13.

Table 13 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Description

Use **rule** to create or edit an IPv6 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

By default, an IPv6 advanced ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** command.

If an IPv6 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify the **fragment** or **routing** keyword, or specify **neq** for the *operator* argument.
- The **logging** and **counting** keywords (even if specified) do not take effect for QoS traffic classification.

Related commands: **acl ipv6**, **display ipv6 acl**, **step**, and **time-range**.

Examples

# Create an IPv6 ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96, and enable logging matching packets.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96
destination-port eq 80 logging
```

# Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule permit ipv6
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
```

# Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
```

# Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3003
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmptrap
```

rule (IPv6 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range**] *

View

IPv6 basic ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv6 ACL rule has been matched in hardware.

fragment: Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

logging: Logs matching packets. This function requires that the module (for example, packet filter) that uses the ACL supports logging.

routing [**type** *routing-type*]: Matches a specific type of routing header or any type of routing header. The *routing-type* argument takes a value in the range of 0 to 255. If no routing header type is specified, the rule matches any type of routing header.

source { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** }: Matches a source IP address. The *ipv6-address* and *prefix-length* arguments represent a source IPv6 address and address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule; however, the rule using the time range can take effect only after you configure the timer range.

Description

Use **rule** to create or edit an IPv6 basic ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

By default, an IPv6 basic ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** command.

Related commands: **acl ipv6**, **display ipv6 acl**, **step**, and **time-range**.

NOTE:

- If an IPv6 basic ACL is for QoS traffic classification, do not specify the **fragment** or **routing** keyword. The keyword can cause ACL application failure. The **logging** and **counting** keywords (even if specified) do not take effect for QoS.
- If an IPv6 basic ACL is for packet filtering, do not specify the **fragment** or **routing** keyword.

Examples

# Create an IPv6 basic ACL rule to deny the packets from any source IP segment but 1001::/16, 3124:1123::/32, or FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 1001:: 16
[Sysname-acl6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl6-basic-2000] rule deny source any
```

rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View

IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default level

2: System level

Parameters

rule-id: Specifies ACL rule ID, in the range of 0 to 65534. The rule must already exist.

text: Adds a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

Description

Use **rule comment** to add a comment about an existing ACL rule or edit its comment to make the rule easy to understand.

Use **undo rule comment** to delete the ACL rule comment.

By default, an IPv4 ACL rule has no rule comment.

Related commands: **display acl** and **display acl ipv6**.

Examples

# Create a rule in IPv4 basic ACL 2000 and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on GigabitEthernet 1/0/1.
```

# Create a rule in IPv6 basic ACL 2000 and add a comment about the rule.

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 1001::1 128
[Sysname-acl6-basic-2000] rule 0 comment This rule is used on GigabitEthernet 1/0/1.
```

rule remark

Syntax

rule [*rule-id*] **remark** *text*

undo rule [*rule-id*] **remark** [*text*]

View

IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule number in the range of 0 to 65534. The specified rule can be one that has been created or not. If you specify no rule ID when adding a remark, the system automatically picks the rule ID that is the nearest higher multiple of the numbering step to the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the system picks rule 30.

text: Specifies a remark, a case-sensitive string of 1 to 63 characters.

Description

Use **rule remark** to add a start or end remark for a range of rules that are created for the same purpose.

Use **undo rule remark** to delete a rule range remark.

By default, no rule range remarks are configured.

A rule range remark always appears immediately above the specified rule. If the specified rule has not been created yet, the position of the comment in the ACL is as follows:

- If the match order is config, the remark is inserted into the ACL in descending order of rule ID.
- If the match order is auto, the remark is placed at the end of the ACL. After you create the rule, the remark appears above the rule.

To display rule range remarks in an ACL, use the **display this** or **display current-configuration**.

When you delete rule range remarks, follow these guidelines:

- If neither *rule-id* nor *text* is specified, all rule range remarks are removed.
- Use the **undo rule remark** *text* command to remove all remarks that are the same as the *text* argument.
- Use the **undo rule** *rule-id* **remark** command to delete a specific rule range remark. If you also specify the *text* argument, you must type in the remark the same as was specified to successfully remove the remark.

TIP:

When adding an end remark for a rule range, you can specify the end rule number plus 1 for the *rule-id* argument so all rules in this range appears between the two remarks. You can also specify the end rule number for the *rule-id* argument. In this approach, the end rule appears below the end remark. Whichever approach you use, be consistent.

Related commands: **display this**, **display current-configuration** (*Fundamentals Command Reference*).

Examples

# Display the running configuration of IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
#
return
```

# Add a start comment "Rules for VIP_start" and an end comment "Rules for VIP_end" for the rule range 10 to 25.

```
[Sysname-acl-basic-2000] rule 10 remark Rules for VIP_start
[Sysname-acl-basic-2000] rule 26 remark Rules for VIP_end
```

# Verify the configuration.

```
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 remark Rules for VIP_start
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
 rule 26 remark Rules for VIP_end
#
return
```

step

Syntax

step *step-value*

undo step

View

IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default level

2: System level

Parameters

step-value: ACL rule numbering step, in the range of 1 to 20.

Description

Use **step** to set a rule numbering step for an ACL. The rule numbering step sets the increment by which the system numbers rules automatically. For example, the default ACL rule numbering step is 5. If you do not assign IDs to rules you are creating, they are numbered 0, 5, 10, 15, and so on. The wider the numbering step, the more rules you can insert between two rules. Whenever the step changes, the rules are renumbered, starting from 0. For example, if there are five rules numbered 5, 10, 13, 15, and 20, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6 and 8.

Use **undo step** to restore the default.

The default rule numbering step is 5. After you restore the default numbering step by the **undo step** command, the rules are renumbered in steps of 5.

Related commands: **display acl** and **display acl ipv6**.

Examples

# Set the rule numbering step to 2 for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

# Set the rule numbering step to 2 for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

time-range

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

View

System view

Default level

2: System level

Parameters

time-range-name: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. It must start with an English letter and to avoid confusion, cannot be **all**.

start-time **to** *end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock), and each value is in the range of 00:00 to 23:59. The end time must be greater than the start time.

days: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, respectively.
- A day of a week in words, **sun**, **mon**, **tue**, **wed**, **thu**, **fri**, and **sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

from *time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value is in the range of 00:00 to 23:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range depending on MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If not specified, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

to *time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00 to 24:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be greater than the start time. If not specified, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

Description

Use **time-range** to configure a time range.

Use **undo time-range** to delete a time range or a statement in the time range.

By default, no time range exists.

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on Monday between January 1, 2010 00:00 and December 31, 2010 23:59, use the **time-range test 08:00 to 12:00 mon from 00:00 01/01/2010 to 23:59 12/31/2010** command.

The active period of a time range is calculated as follows:

1. Combining all periodic statements
2. Combining all absolute statements
3. Taking the intersection of the two statement sets as the active period of the time range

You can create a maximum of 256 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements.

Related commands: **display time-range**.

Examples

# Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range t1 8:0 to 18:0 working-day
```

# Create an absolute time range **t2**, setting it to be active in the whole year of 2010.

```
<Sysname> system-view
[Sysname] time-range t2 from 0:0 1/1/2010 to 23:59 12/31/2010
```

# Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2010.

```
<Sysname> system-view
[Sysname] time-range t3 8:0 to 12:0 off-day from 0:0 1/1/2010 to 23:59 12/31/2010
```

# Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in the period of January through June of the year 2010.

```
<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 23:59 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 23:59 6/30/2010
```

QoS policy configuration commands

Class configuration commands

display traffic classifier

Syntax

display traffic classifier user-defined [*tcl-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined classes.

tcl-name: Class name, a string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display traffic classifier** to display class information.

If no class name is specified, the command displays information about all user-defined classes.

Examples

# Display information about all user-defined classes.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
  Operator: AND
  Rule(s) : if-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : if-match acl 3131
```

Table 14 Command output

Field	Description
Classifier	Class name and its match criteria.
Operator	The match operator you set for the class. If the operator is AND, the class matches the packets that match all its match criteria. If the operator is OR, the class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

View

Class view

Default level

2: System level

Parameters

match-criteria: Specifies a match criterion. Table 15 shows the available criteria.

Table 15 The value range for the *match-criteria* argument

Keyword and argument combination	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The *acl-number* argument ranges from 2000 to 3999 for an IPv4 ACL, 2000 to 3999 for an IPv6 ACL, and 4000 to 4999 for an Ethernet frame header ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter from a to z or A to Z, and to avoid confusion, cannot be **all**.
any	Matches all packets.
dscp *dscp-list*	Matches DSCP values. The *dscp-list* argument is a list of up to eight DSCP values. A DSCP value can be a number from 0 to 63 or any keyword in Table 17.
destination-mac *mac-address*	Matches a destination MAC address.
customer-dot1p *8021p-list*	Matches the 802.1p priority of the customer network. The *8021p-list* argument is a list of up to eight 802.1p priority values. An 802.1p priority ranges from 0 to 7.

Keyword and argument combination	Description
service-dot1p *8021p-list*	Matches the 802.1p priority of the service provider network. The *8021p-list* argument is a list of up to eight 802.1p priority values. An 802.1p priority ranges from 0 to 7.
ip-precedence *ip-precedence-list*	Matches IP precedence. The *ip-precedence-list* argument is a list of up to eight IP precedence values. An IP precedence ranges from 0 to 7.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be IP or IPv6.
source-mac *mac-address*	Matches a source MAC address.
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of customer networks. The *vlan-id-list* argument is a list of up to eight VLAN IDs. The *vlan-id1* **to** *vlan-id2* specifies a VLAN ID range, where the *vlan-id1* must be smaller than the *vlan-id2*. A VLAN ID ranges from 1 to 4094.
service-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of ISP networks. The *vlan-id-list* is a list of up to eight VLAN IDs. The *vlan-id1* **to** *vlan-id2* specifies a VLAN ID range, where the *vlan-id1* must be smaller than the *vlan-id2*. A VLAN ID ranges from 1 to 4094.
system-index *index-value-list*	Matches a pre-defined match criterion (system-index) for packets sent to the control plane. The *index-value-list* argument specifies a list of up to eight system indexes. The system index ranges from 1 to 128.

NOTE:

If a class that uses the AND operator has multiple **if-match acl**, **if-match acl ipv6**, **if-match customer-vlan-id** or **if-match service-vlan-id** clauses, a packet that matches any of the clauses matches the class.

To successfully execute the traffic behavior associated with a traffic class that uses the AND operator, define only one **if-match** clause for any of the following match criteria and input only one value for any of the following *list* arguments, for example, the *8021p-list* argument:

- **customer-dot1p** *8021p-list*
- **destination-mac** *mac-address*
- **dscp** *dscp-list*
- **ip-precedence** *ip-precedence-list*
- **service-dot1p** *8021p-list*
- **source-mac** *mac-address*
- **system-index** *index-value-list*

To create multiple **if-match** clauses for these match criteria or specify multiple values for the *list* arguments, configure the operator of the class as OR and execute the **if-match** command multiple times.

Description

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

When defining match criteria, use the usage guidelines described in these subsections.

Defining an ACL-based match criterion

If the ACL referenced in the **if-match** command does not exist, the class cannot be applied to hardware.

For a class, you can reference an ACL twice by its name and number, respectively, with the **if-match** command.

Defining a criterion to match a destination MAC address

You can configure multiple destination MAC address match criteria for a class.

Defining a criterion to match a source MAC address

You can configure multiple source MAC address match criteria for a class.

Defining a criterion to match DSCP values

- You can configure multiple DSCP match criteria for a class. All defined DSCP values are automatically sorted in ascending order.
- To delete a criterion that matches DSCP values, the specified DSCP values must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match 802.1p priority in customer or service provider VLAN tags

- You can configure multiple 802.1p priority match criteria for a class. All the defined 802.1p values are automatically arranged in ascending order.
- To delete a criterion that matches 802.1p priority values, the specified 802.1p priority values in the command must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match IP precedence values

- You can configure multiple IP precedence match criteria for a class. The defined IP precedence values are automatically arranged in ascending order.
- To delete a criterion that matches IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match customer network VLAN IDs or service provider network VLAN IDs

- You can configure multiple VLAN ID match criteria for a class. The defined VLAN IDs are automatically arranged in ascending order.
- You can configure multiple VLAN IDs in one command line. If the same VLAN ID is specified multiple times, the system considers them as one. If a packet matches one of the defined VLAN IDs, it matches the **if-match** clause.
- To delete a criterion that matches VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (the sequence may be different).

Referencing a pre-define match criterion for packets sent to the control plane

- You can configure multiple match criteria in a class for packets sent to the control plane.
- You can configure multiple system indexes in one command. If the same system index is specified multiple times, the system considers them as one. If a packet matches one of the defined system indexes, it matches the **if-match** clause.

- To delete a criterion that matches system indexes, the specified system indexes in the command must be identical with those defined in the criterion (the sequence may be different).
- You can use the **display qos policy control-plane pre-defined** command to display the pre-defined match criteria for packets sent to the control plane of the switch.

Related commands: **traffic classifier**.

Examples

# Define a match criterion for class **class1** to match the packets with their destination MAC addresses being 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

# Define a match criterion for class **class2** to match the packets with their source MAC addresses being 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

# Define a match criterion for class **class1** to match the packets with their customer network 802.1p priority values being 3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3
```

# Define a match criterion for class **class1** to match the packets with their service provider network 802.1p priority values being 5.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

# Define a match criterion for class **class1** to match the advanced ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

# Define a match criterion for class **class1** to match the ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

# Define a match criterion for class **class1** to match the advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

# Define a match criterion for class **class1** to match the IPv6 ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

# Define a match criterion for class **class1** to match all packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
```

```
[Sysname-classifier-class1] if-match any
```

# Define a match criterion for class **class1** to match the packets with their DSCP values being 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match dscp 1
[Sysname-classifier-class1] if-match dscp 6
[Sysname-classifier-class1] if-match dscp 9
```

# Define a match criterion for class **class1** to match the packets of SVLAN 2, 7, or 10.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

# Define a match criterion for class **class1** to match the packets with their IP precedence values being 1 or 6.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match ip-precedence 1
[Sysname-classifier-class1] if-match ip-precedence 6
```

# Define a match criterion for class **class1** to match the packets of a customer network VLAN of 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

# Define a match criterion for class **class1** to match packets matching the pre-defined system-index 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match system-index 1
```

traffic classifier

Syntax

traffic classifier *tcl-name* [**operator** { **and** | **or** }]

undo traffic classifier *tcl-name*

View

System view

Default level

2: System level

Parameters

tcl-name: Specifies a class name, a string of 1 to 31 characters.

operator: Sets the operator to logic AND or OR for the class.

and: Specifies the logic AND operator. The class matches the packets that match all its criteria.

or: Specifies the logic OR operator. The class matches the packets that match any of its criteria.

Description

Use **traffic classifier** to create a class and enter class view.

Use **undo traffic classifier** to delete a class.

If no match operator is specified, the default AND operator applies.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

# Create a class **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Traffic behavior configuration commands

accounting

Syntax

accounting

undo accounting

View

Traffic behavior view

Default level

2: System level

Parameters

None

Description

Use **accounting** to configure the traffic accounting action in a traffic behavior.

Use **undo accounting** to delete the traffic accounting action from a traffic behavior.

You can use the accounting action to collect statistics for a traffic class, for example, the traffic sourced from a certain IP address.

You can use the **display qos policy interface** command and the **display qos vlan-policy** command to display class-based traffic statistics.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure the accounting action in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

car

Syntax

car **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *action*] [**red** *action*]

undo car

View

Traffic behavior view

Default level

2: System level

Parameters

cir *committed-information-rate*: Specifies the committed access rate (in kbps), which limits the average traffic rate. The CIR ranges from 64 to 10000000, and must be a multiple of 64.

cbs *committed-burst-size*: Specifies the committed burst size (in bytes).

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and cannot not exceed 16000000.
- If you specify the **cbs** keyword, the CBS ranges from 4000 to 16000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The *excess-burst-size* argument ranges from 0 to 16000000, and defaults to 4000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The *peak-information-rate* argument ranges from 64 to 10000000 and must be a multiple of 64.

green *action*: Specifies the action to take on a packet that conforms to CIR. The default is **pass**.

yellow *action*: Specifies the action to take on a packet that conforms to PIR but not to CIR. The default is **pass**.

red *action*: Specifies the action to take on a packet that conforms to neither CIR nor PIR. The default is **discard**.

action: Sets the action to take on the packet:

- **discard**—Drops the packet.
- **pass**—Permits the packet to pass through.
- **remark-dscp-pass** *new-dscp*—Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument ranges from 0 to 63 or is a keyword in Table 17.

Description

Use **car** to configure a CAR action in a traffic behavior.

Use **undo car** to delete a CAR action from a traffic behavior.

You can use a CAR action to rate limit inbound traffic.

A traffic behavior can have only one CAR action. If you configure the **car** command multiple times in a traffic behavior, the last configuration takes effect.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure a CAR action in the traffic behavior **database**:

- Set the CIR to 128 kbps, CBS to 50000 bytes, and EBS to 0.
- Allow the conforming packets to pass, and mark the excess packets with DSCP precedence 0 and forward them.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 128 cbs 50000 ebs 0 green pass red remark-dscp-pass
0
```

display traffic behavior

Syntax

display traffic behavior user-defined [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined traffic behaviors.

behavior-name: Behavior name, a string of 1 to 31 characters. If no traffic behavior is specified, this command displays information about all the user-defined behaviors.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display traffic behavior** to display traffic behavior information.

Examples

# Display user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
    Behavior: 2
      Accounting enable:
      Committed Access Rate:
        CIR 12800 (kbps), CBS 40960 (byte), EBS 4000 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
      Redirect enable:
        Redirect type: cpu
        Redirect destination: cpu
      Marking:
        Remark dot1p COS 1
      Marking:
        Remark DSCP af12
```

Table 16 Command output

Field	Description
User Defined Behavior Information	User-defined behavior information.
Behavior	Traffic behavior name.
Marking	Information about traffic marking.
Remark	Type of precedence marked for traffic, which can be DSCP, IP precedence, dot1p (COS), qos local ID, local precedence, drop precedence, customer VLAN ID or service VLAN ID. For more information about these precedence types, see "Traffic behavior configuration commands."
Accounting enable	Class-based accounting mode.
Committed Access Rate	Information about the CAR action.
Green Action	Action to take on green packets, which can be **pass** or **discard**.
Red Action	Action to take on red packets, which can be **pass** or **discard.**
Redirect enable	Traffic redirecting configuration.
Redirect type	Traffic redirecting type, which can be redirecting traffic to the CPU or an interface.
Redirect destination	Destination for traffic redirecting, which can be an interface name or the CPU.

filter

Syntax

filter { **deny** | **permit** }

undo filter

View

Traffic behavior view

Default level

2: System level

Parameters

deny: Drops packets.

permit: Permits packet to pass through.

Description

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to delete the traffic filtering action.

Examples

# Configure the traffic filtering action as **deny** in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

View

Traffic behavior view

Default level

2: System level

Parameters

cpu: Redirects traffic to the CPU.

interface: Redirects traffic to an interface.

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **redirect** to configure a traffic redirecting action in the traffic behavior.

Use **undo redirect** to delete the traffic redirecting action.

NOTE:

Redirecting traffic to CPU and redirecting traffic to an interface are mutually exclusive with one another in a traffic behavior.

Examples

# Configure redirecting traffic to GigabitEthernet 1/0/1 in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet1/0/1
```

remark dot1p

Syntax

remark dot1p { *8021p* | **customer-dot1p-trust** }

undo remark dot1p

View

Traffic behavior view

Default level

2: System level

Parameters

8021p: 802.1p priority to be marked for packets, which ranges from 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag after the QoS policy is applied to a port. This keyword does not take effect on single-tagged packets.

Description

Use **remark dot1p** to configure an 802.1p priority marking action or configure the inner-to-outer tag priority copying action.

Use **undo remark dot1p** to delete the action.

The **remark dot1p** *8021p* command and the **remark dot1p customer-dot1p-trust** command override each other, whichever is configured the last.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure traffic behavior **database** to mark matching traffic with 802.1p priority 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

# Configure the inner-to-outer tag priority copying action in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p customer-dot1p-trust
```

remark drop-precedence

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

drop-precedence-value: Drop precedence to be marked for packets. The value range is 0 to 2. The switch preferentially drops packets with the highest drop precedence.

Description

Use **remark drop-precedence** to configure a drop precedence marking action.

Use **undo remark drop-precedence** to delete the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure traffic behavior **database** to mark matching traffic with drop precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

remark dscp

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo remark [**green** | **red** | **yellow**] **dscp**

View

Traffic behavior view

Default level

2: System level

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: DSCP value, which can be a number from 0 to 63 or any keyword in Table 17.

Table 17 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24

Keyword	DSCP value (binary)	DSCP value (decimal)
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

Description

Use **remark dscp** to configure a DSCP marking action.

Use **undo remark dscp** to delete the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure the traffic behavior **database** to mark matching traffic with DSCP 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark ip-precedence

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

ip-precedence-value: IP precedence value to be marked for packets, which ranges from 0 to 7.

Description

Use **remark ip-precedence** to configure an IP precedence marking action.

Use **undo remark ip-precedence** to delete the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Set the IP precedence to 6 for packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

remark local-precedence

Syntax

remark local-precedence *local-precedence*

undo remark local-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

local-precedence: Sets the local precedence to be marked for packets, which ranges from 0 to 7.

Description

Use **remark local-precedence** to configure a local precedence marking action.

Use **undo remark local-precedence** to delete the action.

If a traffic behavior has both **remark local-precedence** and **remark dot1p** actions, the re-marked local precedence and 802.1p priority must be the same for the class-behavior association to be successfully applied.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

# Configure traffic behavior **database** to mark matching traffic with local precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default level

2: System level

Parameters

behavior-name: Sets a behavior name, a string of 1 to 31 characters.

Description

Use **traffic behavior** to create a traffic behavior and enter traffic behavior view.

Use **undo traffic behavior** to delete a traffic behavior.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

# Create a traffic behavior named **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

QoS policy configuration and application commands

classifier behavior

Syntax

classifier *tcl-name* **behavior** *behavior-name*

undo classifier *tcl-name*

View

Policy view

Default level

2: System level

Parameters

tcl-name: Class name, a string of 1 to 31 characters.

behavior-name: Behavior name, a string of 1 to 31 characters.

Description

Use **classifier behavior** to associate a behavior with a class in a QoS policy.

Use **undo classifier** to remove a class from the policy.

You can perform a set of QoS actions on a traffic class by associating a traffic behavior with the traffic class.

You can configure multiple class-behavior associations in a QoS policy, and each class can associate with only one traffic behavior.

If the specified class or traffic behavior does not exist, the system creates a null class or traffic behavior.

Related commands: **qos policy**.

Examples

# Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
[Sysname-qospolicy-user1]
```

control-plane

Syntax

control-plane slot *slot-number*

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Enter the control plane view of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the switches in the IRF fabric.

Description

Use **control-plane** to enter control plane view.

Examples

# Enter the control plane view of IRF member 2.

```
<Sysname> system-view
[Sysname] control-plane 2
[Sysname-cp-slot2]
```

display qos policy

Syntax

display qos policy user-defined [*policy-name* [**classifier** *tcl-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined QoS policies.

policy-name: QoS policy name, a string of 1 to 31 characters. If no policy is specified, this command displays configuration information of all the policies.

tcl-name: Class name, a string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos policy** to display user-defined QoS policy configuration information.

Examples

# Display the configuration information of user-defined QoS policies.

```
<Sysname> display qos policy user-defined
User Defined QoS Policy Information:
Policy: test
 Classifier: 1
   Behavior: be
-none-

 Classifier: USER1
   Behavior: USER1
    Committed Access Rate:
      CIR 256 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Green Action: pass
      Red  Action: discard
    Marking:
      Remark IP Precedence 3
```

Table 18 Command output

Field	Description
Policy	Policy name.
Classifier	Class name. A policy can have multiple classes, and each class is associated with a traffic behavior. A class can have multiple match criteria. For more information, see the **traffic classifier** command in "Class configuration commands."
Behavior	Behavior associated with the class. A behavior specifies a set of actions to take on the traffic that matches the associated class. For more information, see the **traffic behavior** command in "Traffic behavior configuration commands."

display qos policy control-plane

Syntax

display qos policy control-plane slot *slot-number* [**inbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays information about the QoS policy or policies applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

inbound: Displays information about the QoS policy applied in the inbound direction of the control plane.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos policy control-plane** to display information about the QoS policy or policies applied to the specified control plane.

Examples

# Display information about the inbound QoS policy for the control plane of IRF member 3.

```
<Sysname> display qos policy control-plane slot 3 inbound
Control-plane slot 3
  Direction: Inbound
  Policy: 1
    Classifier: 2
      Operator: AND
      Rule(s) : If-match system-index 10
      Behavior: 2
        Committed Access Rate:
          CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
          Red Action: discard
          Green : 12928(Bytes)
          Red   : 43904(Bytes)
        Filter Enable: deny
```

Table 19 Command output

Field	Description
Control-plane	Control plane.
Direction	Direction in which the policy is applied. Only the inbound direction is supported.
Policy	Policy name and its contents.
Classifier	Class name and its contents.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the behavior, and the actions configured in the behavior.
Committed Access Rate	Information about CAR.
CIR	Committed information rate (CIR) in kbps.
CBS	Committed burst size in bytes, which specifies the depth of the token bucket for holding bursty traffic.

Field	Description
EBS	Excessive burst size (EBS) in bytes, which specifies the traffic exceeding CBS when two token buckets are used.
Red Action	Action to take on red packets.
Green	Statistics about green packets.
Red	Statistics about red packets.
Filter Enable	Information about packet filtering (deny indicates dropping packets, and permit indicates forwarding packets).
none	Indicates no other behavior is configured.

display qos policy control-plane pre-defined

Syntax

display qos policy control-plane pre-defined [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays information about the pre-defined QoS policy applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos policy control-plane pre-defined** to display information about the pre-defined QoS policy applied to the control plane.

If no IRF member ID is specified, this command displays information about the pre-defined QoS policy applied to the control plane of each member switch in the IRF fabric.

Examples

# Display information about the pre-defined QoS policy applied to the control plane of IRF member 2.

```
<Sysname> display qos policy control-plane pre-defined slot 2
=================================================================
 Pre-defined Control-plane Policy Slot 2
-----------------------------------------------------------------
```

```
  Index |    PacketType              |  Priority  |  BandWidth(Kbps)
--------------------------------------------------------------------
  1          ISIS                       4            256
  29         ARP                        1            64
  30         ARP_REPLY                  1            64
  35         DOT1X                      1            64
  36         STP                        6            128
  37         LACP                       5            64
  38         GVRP                       3            256
  41         ICMP                       1            0
  53         LLDP                       3            64
  54         DLDP                       3            64
=================================================================
```

Table 20 Command output

Field	Description
Pre-defined Control-plane Policy	Contents of the pre-defined control plane QoS policy
Index	Pre-defined system index
PacketType	Match criterion

display qos policy global

Syntax

display qos policy global [**slot** *slot-number*] [**inbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Displays information about the inbound global QoS policy. An inbound global QoS policy applies to the inbound direction of all ports.

slot *slot-number*: Displays the global QoS policy configuration of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos policy global** to display information about global QoS policies.

If the *slot-number* argument is not specified, the global QoS policy configuration of all devices in the IRF fabric is displayed.

Examples

# Display information about the inbound global QoS policy.

```
<Sysname> display qos policy global

Direction: Inbound

  Policy: 1
   Classifier: 2
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 2
       Accounting Enable
         20864 (Packets)
       Committed Access Rate:
         CIR 128 (kbps), CBS 8000 (Bytes), EBS 0 (Bytes)
         Red Action: discard
         Green : 12928(Packets)
         Red   : 43904(Packets)
```

Table 21 Command output

Field	Description
Direction	Direction in which the policy is applied globally
Policy	Policy name and its contents.
Classifier	The name and content of a class. If the switch has failed to apply the class-behavior association, the field displays "**(Failed)**" behind the class name. In an IRF fabric: • If the **display** command is executed without any member switch specified, "**(Failed)**" indicates that the class-behavior association has failed to apply to the IRF fabric globally. • If a member switch is specified, "**(Failed)**" indicates that the class-behavior association has failed to apply to the specified IRF member switch. The failure to apply one class-behavior association does not affect the application of other associations in the QoS policy.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the traffic behavior, and the actions in the traffic behavior.

display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number to display information about the QoS policy or policies applied to it.

inbound: Displays information about the QoS policy applied in the inbound direction of the specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos policy interface** to display information about the QoS policy or policies applied to an interface or all interfaces.

Examples

# Display information about the QoS policy or policies applied to GigabitEthernet1/0/1.

```
<Sysname> display qos policy interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Accounting Enable:
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/2
      Redirect enable:
        Redirect type: cpu
        Redirect destination: cpu
      Marking:
        Remark Customer VLAN ID 100
      Marking:
```

```
    Remark dot1p COS 2
  Marking:
    Remark IP precedence 3
  Marking:
    Remark qos local ID 3
```

Table 22 Command output

Field	Description
Interface	Interface type and interface number
Direction	Direction in which the policy is applied to the interface
Policy	Name of the policy applied to the interface
Classifier	Class name and configuration information
Operator	Logical relationship between match criteria in the class
Rule(s)	Match criteria in the class
Behavior	Behavior name and configuration information

display qos vlan-policy

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

name *policy-name*: Displays information about the VLAN QoS policy specified by its name, a string of 1 to 31 characters.

vlan *vlan-id*: Displays information about the QoS policy or policies applied to the VLAN specified by its ID.

inbound: Displays information about the QoS policy applied to the inbound direction of the specified VLAN.

slot *slot-number*: Displays the VLAN QoS policy information of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos vlan-policy** to display VLAN QoS policy information.

If no member switch is specified, this command displays VLAN QoS policy information for the IRF fabric.

Examples

# Display information about the VLAN QoS policy **test** on IRF member switch 3.

```
<Sysname> display qos vlan-policy name test slot 3
  Policy test
    Vlan 200: inbound
```

Table 23 Command output

Field	Description
Policy	Name of the QoS policy.
Vlan	ID of the VLAN where the VLAN policy is applied.
inbound	The QoS policy is applied in the inbound direction of the VLAN.

# Display information about the QoS policies applied to VLAN 2.

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2

Direction: Inbound

  Policy: 1
   Classifier: 2
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 2
       Accounting Enable
         163 (Packets)
       Committed Access Rate:
         CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
         Red Action: discard
         Green : 12928(Packets)
         Red   : 43904(Packets)
```

Table 24 Command output

Field	Description
Vlan	ID of the VLAN where the QoS policy is applied.
Direction	Direction in which the QoS policy is applied for the VLAN.

Field	Description
Classifier	The name and content of a class. If the switch has failed to apply the class-behavior association, the field displays "**(Failed)**" after the class name. In an IRF environment: • If you specify the **slot** keyword in the display command, "**(Failed)**" indicates that the class-behavior association has failed to be applied to the IRF fabric. • If the **slot** keyword is not specified, "**(Failed)**" indicates that the class-behavior association has failed to be applied to the specified IRF member switch. A QoS policy can comprise multiple class-behavior associations. The failure to apply one class-behavior association does not affect the others.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the behavior, and its actions.

qos apply policy (interface view, port group view, control plane view)

Syntax

qos apply policy *policy-name* **inbound**

undo qos apply policy [*policy-name*] **inbound**

View

Layer 2 Ethernet interface view, port group view, control plane view

Default level

2: System level

Parameters

inbound: Inbound direction.

policy-name: Specifies a policy name, a string of 1 to 31 characters.

Description

Use **qos apply policy** to apply a QoS policy.

Use **undo qos apply policy** to remove the QoS policy.

Examples

# Apply policy **USER1** in the inbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy USER1 inbound
```

# Apply policy **aaa** to the inbound direction of the switch numbered 3 in the IRF fabric.

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3] qos apply policy aaa inbound
```

qos apply policy (user-profile view)

Syntax

qos apply policy *policy-name* **inbound**

undo qos apply policy [*policy-name*] **inbound**

View

User profile view

Default level

2: System level

Parameters

inbound: Applies the QoS policy to the traffic sent by the online users.

policy-name: Policy name, a string of 1 to 31 characters.

Description

Use **qos apply policy** to apply a QoS policy to a user profile.

Use **undo qos apply policy** to remove the QoS policy.

If a user profile is activated, the QoS policy, including the ACLs referenced in the QoS policy, applied to it cannot be configured or removed.

The QoS policy applied to a user profile takes effect when the user-profile is activated and the users are online.

Only the **remark**, **car**, and **filter** actions are supported in the QoS policies applied in user profile view.

A null policy cannot be applied in user profile view.

Examples

# Apply policy **test** to the traffic sent by the users online. (Assume that that the QoS policy has been configured.)

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test inbound
```

qos apply policy global

Syntax

qos apply policy *policy-name* **global inbound**

undo qos apply policy [*policy-name*] **global inbound**

View

System view

Default level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming packets on all ports.

Description

Use **qos apply policy global** to apply a QoS policy globally. A global QoS policy takes effect on all inbound traffic.

Use **undo qos apply policy global** to remove the QoS policy.

Examples

# Apply the QoS policy **user1** in the inbound direction globally.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view

Default level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 31 characters.

Description

Use **qos policy** to create a policy and enter policy view.

Use **undo qos policy** to delete a policy.

To use the **undo qos policy** command to delete a policy that has been applied to a certain object, you must first remove it from the object.

Related commands: **classifier behavior**, **qos apply policy**, **qos apply policy global**, and **qos vlan-policy**.

Examples

# Define QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

qos vlan-policy

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* **inbound**

undo qos vlan-policy [*policy-name*] **vlan** *vlan-id-list* **inbound**

View

System view

Default level

2: System level

Parameters

policy-name: QoS policy name, a string of 1 to 31 characters.

vlan-id-list: Specifies a list of up to eight VLAN IDs. A VLAN ID ranges from 1 to 4094. You can input individual discontinuous VLAN IDs and VLAN ID ranges in the form of *start-vlan-id* **to** *end-vlan-id* where the start VLAN ID must be smaller than the end VLAN ID. Each item in the VLAN list is separated by a space.

inbound: Applies the QoS policy to the incoming packets in the specified VLAN(s).

Description

Use **qos vlan-policy** to apply a QoS policy to VLANs.

Use **undo qos vlan-policy** to remove the QoS policy applied to VLANs.

Examples

# Apply the QoS policy **test** to the inbound direction of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

reset qos policy control-plane

Syntax

reset qos policy control-plane slot *slot-number* [**inbound**]

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the statistics of the QoS policy or policies applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

inbound: Clears the statistics of the QoS policy applied to the inbound direction of the control plane.

Description

Use **reset qos policy control-plane** to clear the statistics of the QoS policy applied in the inbound direction of a control plane.

Examples

# Clear statistics for the inbound QoS policy of the control plane on IRF member 3.

```
<Sysname> reset qos policy control-plane slot 3 inbound
```

reset qos policy global

Syntax

reset qos policy global [**inbound**]

View

User view

Default level

1: Monitor level

Parameters

inbound: Specifies the inbound direction.

Description

Use **reset qos policy global** to clear the statistics of a global QoS policy.

Examples

# Clear the statistics of the global QoS policy in the inbound direction.

```
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound**]

View

User view

Default level

1: Monitor level

Parameters

vlan-id: VLAN ID, which ranges from 1 to 4094.

inbound: Clears the statistics of the QoS policy applied in the inbound direction of the specified VLAN.

Description

Use **reset qos vlan-policy** to clear the statistics of the QoS policy applied in a certain direction of a VLAN.

Examples

# Clear the statistics of QoS policies applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

Priority mapping configuration commands

Priority mapping table configuration commands

display qos map-table

Syntax

display qos map-table [**dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dot1p-dp: 802.1p-to-drop mapping table.

dot1p-lp: 802.1p-to-local mapping table.

dscp-dot1p: DSCP-to-802.1p mapping table.

dscp-dp: DSCP-to-drop mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos map-table** to display the configuration of a priority mapping table.

If no priority mapping table is specified, this command displays the configuration information of all priority mapping tables.

Related commands: **qos map-table**.

Examples

# Display the configuration of the 802.1p-to-local mapping table.

```
<Sysname> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

# Display the configuration information of the 802.1p-to-drop mapping table.

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-dp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    0
   1    :    0
   2    :    0
   3    :    0
   4    :    0
   5    :    0
   6    :    0
   7    :    0
```

Table 25 Command output

Field	Description
MAP-TABLE NAME	Name of the priority mapping table
TYPE	Type of the priority mapping table
IMPORT	Input values of the priority mapping table
EXPORT	Output values of the priority mapping table

import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

View

Priority mapping table view

Default level

2: System level

Parameters

import-value-list: List of input values.

export-value: Output value.

all: Deletes all the mappings in the priority mapping table.

Description

Use **import** to configure a mapping from one or multiple input values to an output value.

Use **undo import** to restore the specified or all mappings to the default mappings.

Related commands: **display qos map-table**.

Examples

# Configure the 802.1p-to-drop mapping table to map 802.1p priority values 4 and 5 to drop precedence 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```

qos map-table

Syntax

qos map-table { **dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** }

View

System view

Default level

2: System level

Parameters

dot1p-dp: 802.1p-to-drop mapping table.

dot1p-lp: 802.1p-to-local mapping table.

dscp-dot1p: DSCP-to-802.1p mapping table.

dscp-dp: DSCP-to-drop mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

Description

Use **qos map-table** to enter the specified priority mapping table view.

Related commands: **display qos map-table**.

Examples

# Enter the 802.1p-to-drop mapping table view.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

Port priority configuration commands

qos priority

Syntax

qos priority *priority-value*

undo qos priority

View

Interface view, port group view

Default level

2: System level

Parameters

priority-value: Port priority value, in the range of 0 to 7.

Description

Use **qos priority** to change the port priority of an interface.

Use **undo qos priority** to restore the default.

The default port priority is 0.

You can use the **display qos trust interface** command to view the port priority of an interface.

When a switch receives an untagged packet on an interface, the switch uses the port priority of the interface as the 802.1p priority of the received packet, and then looks up the 802.1p-to-local and 802.1p-to-drop priority mapping tables and mark the packet with the corresponding local precedence and drop precedence.

Examples

# Set the port priority of interface GigabitEthernet 1/0/1 to 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

Port priority trust mode configuration commands

display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos trust interface** to display priority trust mode and port priority information on an interface.

If no interface is specified, the command displays priority trust mode and port priority information for all interfaces.

Examples

# Display the priority trust mode and port priority settings of GigabitEthernet 1/0/1.

```
<Sysname> display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority :0
  Port priority trust type : dscp
```

Table 26 Command output

Field	Description
Interface	Interface type and interface number
Port priority	Port priority set for the interface
Port priority trust type	Priority trust mode on the interface: • **dscp**—Uses the DSCP precedence of incoming packets for priority mapping. • **dot1p**—Uses the 802.1p priority of incoming packets for priority mapping. • **untrust**—Uses the port priority for priority mapping.

qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

View

Interface view, port group view

Default level

2: System level

Parameters

dot1p: Uses the 802.1p priority in incoming packets for priority mapping.

dscp: Uses the DSCP value in incoming packets for priority mapping.

Description

Use **qos trust** to configure an interface to use a particular priority field carried in packets for priority mapping.

Use **undo qos trust** to restore the default priority trust mode.

By default, the port priority of the incoming interface is used for priority mapping.

In interface view, the setting takes effect on the current interface only. In port group view, the setting takes effect on all ports in the port group.

Examples

# Set the trusted packet priority type to DSCP priority on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

GTS and line rate configuration commands

GTS configuration commands

display qos gts interface

Syntax

display qos gts interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos gts interface** to view generic traffic shaping (GTS) configuration information and operational statistics on a specified interface or all the interfaces.

If no interface is specified, this command displays the GTS configuration information and operational statistics on all the interfaces.

Examples

# Display the GTS configuration information and operational statistics on all the interfaces.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 2
 CIR 640 (kbps), CBS 40960 (byte)
```

Table 27 Command output

Field	Description
Interface	Interface type and interface number
Rule(s)	Match criteria

Field	Description
CIR	Committed information rate (CIR) in kbps
CBS	Committed burst size in bytes, which specifies the depth of the token bucket for holding bursty traffic

qos gts

Syntax

qos gts queue *queue-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-number*

View

Interface view, port group view

Default level

2: System level

Parameters

queue *queue-number*: Shapes the packets in the specified queue. The *queue-number* argument ranges from 0 to 7.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The value range for *committed-information-rate* varies by interface type:

- On a GE port, the argument ranges from 64 to 1000000, and must be a multiple of 64.
- On a 10-GE port, the argument ranges from 64 to 10000000, and must be a multiple of 64.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes.

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and must be a multiple of 4096. If 62.5 × *committed-information-rate* is not a multiple of 4096, the closest higher multiple of 4096 applies. The CBS cannot exceed 16777216.
- If you specify the **cbs** keyword, the CBS ranges from 4096 to 16777216 and must be a multiple of 4096.

Description

Use **qos gts** to set GTS parameters for the traffic of the specified queue on the interface or port group.

Use **undo qos gts** to remove GTS parameters for the traffic of the specified queue on the interface or port group.

By default, no GTS parameters are configured on a port.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Examples

# Configure GTS on interface GigabitEthernet 1/0/1 to limit the traffic rate to 640 kbps for queue 2.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts queue 2 cir 640
```

Line rate configuration commands

display qos lr interface

Syntax

display qos lr interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos lr interface** to view the line rate configuration information on a specified interface or all the interfaces.

If no interface is specified, this command displays the line rate configuration information on all the interfaces.

Examples

# Display the line rate configuration information on all the interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 64000 (kbps),  CBS 4000000 (byte)
```

Table 28 Command output

Field	Description
Interface	Interface type and interface number
Direction	Direction in which the line rate configuration is applied
CIR	Committed information rate (CIR) in kbps
CBS	Committed burst size (CBS) in bytes, which specifies the depth of the token bucket for holding bursty traffic

qos lr

Syntax

qos lr outbound cir *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr outbound

View

Interface view, port group view

Default level

2: System level

Parameters

outbound: Limits the rate of outgoing packets on the interface.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The value range for *committed-information-rate* varies by interface type:

- On a GE port, the argument ranges from 64 to 1000000, and must be a multiple of 64.
- On a 10-GE port, the argument ranges from 64 to 10000000, and must be a multiple of 64.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes.

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and must be a multiple of 4000. If 62.5 × *committed-information-rate* is not a multiple of 4000, the closest higher multiple of 4000 applies. The CBS cannot exceed 16000000.
- If you specify the **cbs** keyword, the CBS ranges from 4000 to 16000000 and must be a multiple of 4000.

Description

Use **qos lr** to limit the rate of outgoing packets on the port.

Use **undo qos lr** to remove the rate limit.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Examples

# Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 640 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

Congestion management configuration commands

SP queuing configuration commands

display qos sp

Syntax

display qos sp interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos sp interface** to view the strict priority (SP) queuing configuration of an interface.

If no interface is specified, this command displays the SP queuing configuration of all the interfaces.

Related commands: **qos sp**.

Examples

# Display the SP queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos sp interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Strict-priority queue
```

Table 29 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.

Field	Description
Strict-priority queue	SP queuing is used for queue scheduling.

qos sp

Syntax

qos sp

undo qos sp

View

Interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **qos sp** to configure SP queuing on a port.

Use **undo qos sp** to restore the default.

The default queuing algorithm on a port is WRR queuing.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Related commands: **display qos sp interface**.

Examples

# Enable SP queuing pattern 1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

WRR queuing configuration commands

display qos wrr interface

Syntax

display qos wrr interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos wrr interface** to display the weighted round robin (WRR) queuing configuration on an interface.

If no interface is specified, this command displays the WRR queuing configuration of all the interfaces.

Related commands: **qos wrr**.

Examples

# Display the WRR queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted round robin queue
Queue ID    Group    Weight
-------------------------------------
   0         1        1
   1         sp       N/A
   2         1        3
   3         1        4
   4         1        5
   5         1        6
   6         1        7
   7         1        8
```

Table 30 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.
Queue ID	ID of a queue.
Group	Number of the group a queue is assigned to: • **1**—WRR group • **sp**—SP group
Weight	Queue weight based on which queues are scheduled. **N/A** indicates that the queue uses the SP queue scheduling algorithm.

qos wrr

Syntax

qos wrr

undo qos wrr

View

Interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **qos wrr** to enable WRR queuing.

Use **undo qos wrr** to restore the default scheduling weight.

The default queuing algorithm on a port is WRR queuing.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Examples

# Enable WRR queuing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

qos wrr group sp

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id* **group sp**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

sp: Specifies strict priority (SP) queuing.

Description

Use **qos wrr group sp** to assign a queue to the strict priority (SP) group on a WRR-enabled interface.

Use **undo qos wrr group sp** to remove a queue from the SP group on a WRR-enabled interface.

The Switch Series provides eight output queues per port. You can assign some queues on a port to the SP scheduling group and the others to the WRR scheduling group (group 1) to implement SP+WRR queuing. The switch schedules packets in the SP scheduling group preferentially, and when the SP scheduling group is empty, schedules the packets in the WRR scheduling group. Queues in the SP scheduling group are scheduled with the SP queue scheduling algorithm. Queues in the WRR scheduling group are scheduled with WRR.

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has strict higher scheduling priority than the WRR groups.

Settings in Ethernet interface view take effect on the current interface only. Settings in port group view take effect on all the ports in the port group.

Related commands: **display qos wrr interface** and **qos wrr**.

Examples

# Enable WRR queuing on GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
```

qos wrr weight

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id* **group 1 weight**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Queue ID, which ranges from 0 to 7.

1: Assigns the queue to group 1, the WRR queuing group.

weight *schedule-value*: Specifies a scheduling weight for the specified queue in WRR queuing. The *schedule-value* argument ranges from 1 to 15.

Description

Use **qos wrr weight** to assign a queue to a WRR group, with a certain scheduling weight, on an interface that performs WRR queuing.

Use **undo qos wrr weight** to restore the default WRR queuing settings of a queue on an interface that performs WRR queuing.

By default, the weights of queues 0 through 7 are 1, 2, 3, 4, 5, 9, 13, and 15 on an interface that performs WRR queuing.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Related commands: **display qos wrr interface** and **qos wrr**.

Examples

# Enable WRR queuing on GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10, to WRR group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

WFQ configuration commands

display qos wfq interface

Syntax

display qos wfq interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display qos wfq interface** to display the weighted fair queuing (WFQ) configuration on an interface.

If no interface is specified, this command displays the WFQ configuration of all the interfaces.

Related commands: **qos wfq**.

Examples

# Display the WFQ configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos wfq interface gigabitethernet 1/0/-1
Interface: GigabitEthernet1/0/1
 Output queue: Hardware weighted fair queue
Queue ID        Group           Byte-count      Min-Bandwidth
----------------------------------------------------------------
0                1               1               64
1                1               1               64
2                1               1               64
```

```
3                 1                1                64
4                 1                1                64
5                 1                1                64
6                 1                1                64
7                 1                1                64
```

Table 31 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.
Queue ID	ID of a queue.
Group	Number of the group a queue is assigned to: • **1**—WFQ group • **sp**—SP group
Byte-count	Scheduling weight of the queue in byte-count WFQ, which assigns bandwidth to queues in terms of bytes. If you enable packet-based WFQ on the interface, this field is replaced with **Weight**. For queues in the SP group, **NA** is displayed.
Min-Bandwidth	Minimum guaranteed bandwidth.

qos bandwidth queue

Syntax

qos bandwidth queue *queue-id* **min** *bandwidth-value*

undo qos bandwidth queue *queue-id* [**min** *bandwidth-value*]

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Queue ID, ranging from 0 to 7.

min *bandwidth-value*: Sets the minimum guaranteed bandwidth (in kbps) for a queue when the port is congested. This argument ranges from 64 to 1000000 for a GE port and 64 to 10000000 for a 10-GE port.

Description

Use **qos bandwidth queue** to set the minimum guaranteed bandwidth for a specified queue on the port/port group.

Use **undo qos bandwidth queue** to cancel the configuration.

By default, the minimum guaranteed bandwidth is 64 kbps for a queue.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Configure minimum guaranteed bandwidth only for queues of WFQ-enabled ports.

Examples

# Set the minimum guaranteed bandwidth to 100 kbps for queue 0 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 0 min 100
```

qos wfq

Syntax

qos wfq [**byte-count** | **weight**]

undo qos wfq

View

Interface view, port group view

Default level

2: System level

Parameters

byte-count: Enables byte-count WFQ, which allocates bandwidth to queues in terms of bytes.

weight: Enables packet-based WFQ, which allocates bandwidth to queues in terms of packets.

Description

Use **qos wfq** to enable WFQ on a port.

Use **undo qos wfq** to restore the default queuing algorithm on a port.

The default queuing algorithm on a port is WRR queuing.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

You must enable WFQ before you can configure WFQ queuing parameters for a queue on an interface.

Examples

# Enable byte-count WFQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq byte-count
```

qos wfq byte-count

Syntax

qos wfq *queue-id* **group 1 byte-count** *schedule-value*

undo qos wfq *queue-id* **group 1 byte-count**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

group 1: Assigns a queue to the WFQ group.

byte-count *schedule-value*: Specifies a scheduling weight for the specified queue in byte-count WFQ queuing. The scheduling weight ranges from 1 to 15. On a 5120 EI switch, each scheduling weight corresponds to a scheduling unit, which specifies the number of bytes that can be scheduled from the queue in a cycle of queue scheduling. Table 32 shows the scheduling weight-to-scheduling unit map.

Table 32 The scheduling weight-to-scheduling unit map on a 5120 EI switch

Scheduling weight	Scheduling unit
1	10 KB
2	20 KB
3	40 KB
4	80 KB
5	160 KB
6	320 KB
7	640 KB
8	1280 KB
9	2560 KB
10	5120 KB
11	10 MB
12	20 MB
13	40 MB
14	80 MB
15	160 MB

Description

Use **qos wfq byte-count** to assign a queue to a WFQ group, with a certain scheduling weight, on an interface that performs byte-count WFQ queuing.

Use **undo qos wfq byte-count** to restore the default on an interface that performs byte-count WFQ queuing.

By default, the scheduling weights of queues 0 through 7 are all 1 on an interface that performs byte-count WFQ queuing.

Before using this command on an interface, make sure that the interface is enabled with byte-count WFQ queuing. Otherwise, the weight configuration does not take effect.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Related commands: **display qos wfq interface** and **qos wfq**.

Examples

# Enable byte-count WFQ on interface GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq byte-count
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group 1 byte-count 10
```

qos wfq group sp

Syntax

qos wfq *queue-id* **group sp**

undo qos wfq *queue-id* **group sp**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

sp: Specifies strict priority (SP) queuing.

Description

Use **qos wfq group sp** to assign a queue to the strict priority (SP) group on an interface that performs SP+WFQ queuing.

Use **undo qos wfq group sp** to remove a queue from the SP group on an interface that performs SP+WFQ queuing.

This command is available only on a WFQ-enabled interface. Queues in the SP group are scheduled with SP, instead of WFQ.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Related commands: **display qos wfq interface** and **qos wfq**.

Examples

# Enable WFQ on interface GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group sp
```

qos wfq weight

Syntax

qos wfq *queue-id* **group 1 weight** *schedule-value*

undo qos wfq *queue-id* **group 1 weight**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

group 1: Assigns a queue to the WFQ group.

weight *schedule-value*: Specifies a scheduling weight for the specified queue. The scheduling weight ranges from 1 to 15.

Description

Use **qos wfq weight** to assign a queue to a WFQ group, with a certain scheduling weight, on an interface that performs packet-based WFQ queuing.

Use **undo qos wfq weight** to restore the default WFQ settings of a queue on an interface that performs packet-based WFQ queuing.

By default, the scheduling weights of queues 0 through 7 are all 1 on an interface that performs packet-based WFQ queuing.

Before configuring this command, make sure that the interface is enabled with packet-based WFQ queuing. Otherwise, the weight configuration does not take effect.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

Related commands: **display qos wfq interface**, **qos bandwidth queue**, and **qos wfq**.

Examples

# Enable packet-based WFQ on GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq weight
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group 1 weight 10
```

Data buffer configuration commands

Automatic data buffer configuration commands

burst-mode enable

Syntax

burst-mode enable

undo burst-mode enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **burst-mode enable** to enable the burst function.

Use **undo burst-mode enable** to disable the burst function.

By default, the burst function is disabled.

The burst function allows the switch to automatically determine the shared resource size, the minimum guaranteed resource size for each queue, the maximum shared resource size for each queue, and the maximum shared resource size per port. The function helps optimize the packet buffering scheme to ameliorate forwarding performance.

NOTE:

The **burst-mode enable** command is mutually exclusive with any manual data buffer configuration commands.

Examples

# Enable the burst function.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

Manual data buffer configuration commands

△ CAUTION:

- Data buffer configuration is complicated and has significant impacts on the forwarding performance of a device. Do not modify the data buffer parameters unless you are sure that your device will benefit from the change. If a larger buffer is needed, enable the burst function to allocate buffer automatically.
- The commands in this section are mutually exclusive with the **burst-mode enable** command.

buffer apply

Syntax

buffer apply

undo buffer apply

View

System view

Default level

2: System level

Parameters

None

Description

Use **buffer apply** to apply the configured data buffer settings.

Use **undo buffer apply** to restore the default.

Table 33 shows the default data buffer allocation schemes of the 5120 EI Switch Series.

Table 33 Default data buffer allocation schemes

Resource type	Shared resource size in percentage	Minimum guaranteed resource size per queue in percentage	Maximum shared resource size per port in percentage
Cell resource	50%	12%	50%
Packet resource	N/A	51% for queue 2 and 7% for any other queue.	N/A

Examples

# Apply the data buffer settings.

```
<Sysname> system-view
[Sysname] buffer apply
```

buffer egress queue guaranteed

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone switch, the *slot-number* argument can only be 1. In an IRF fabric, if an IRF member switch is specified, this command applies only to the member switch; if no member switch is specified, this command applies to all member switches.

cell: Configures the minimum guaranteed resource size for a queue in the cell resource.

packet: Configures the minimum guaranteed resource size for a queue in the packet resource.

queue-id: Specifies a queue ID, in the range of 0 to 7.

ratio: Sets the minimum guaranteed resource size for the specified queue as a percentage of the dedicated buffer per port. The value range is 0 to 100.

Description

Use **buffer egress queue guaranteed** to configure the minimum guaranteed resource size for a queue in the cell resource or packet resource.

Use **undo buffer egress queue guaranteed** to restore the default.

By default, the minimum guaranteed resource size for a queue is 12% of the dedicated buffer of the port in the cell resource; the minimum guaranteed resource size is 51% for queue 2 and 7% for any other queue in the packet resource.

The minimum guaranteed resource settings apply to the queue with the same number on each port.

The dedicated resource of a port is shared by eight queues. After you change the minimum guaranteed resource size for a queue, the switch will automatically allocate the remaining dedicated resource among all queues that are not manually assigned a minimum guaranteed resource space. For example, if you set the minimum guaranteed resource size to 30% for a queue, the other seven queues will each share 10% of the remaining dedicated resource of the port.

Examples

# Set 20% of the dedicated buffer per port as the minimum guaranteed resource for queue 0 in the cell resource.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

# In an IRF, set 15% of the dedicated buffer per port as the minimum guaranteed resource for queue 0 in the cell resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell queue 0 guaranteed ratio 15
```

buffer egress shared

Syntax

buffer egress [**slot** *slot-number*] **cell shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell shared**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone device, the *slot-number* argument can only be 1. In an IRF, with *slot-number* specified, this command configures the buffer resource of the member switch specified by *slot-number*; without *slot-number* specified, this command configures the buffer resource of all the member switches in the IRF fabric.

cell: Configures the maximum shared resource size per port in the cell resource.

ratio: Sets the maximum shared resource size per port as a percentage of the shared resource in the range of 0 to 100.

Description

Use **buffer egress shared** to configure the maximum shared resource size per port in the cell resource or packet resource.

Use **undo buffer egress shared** to restore the default.

By default, the maximum shared resource size per port is 50% of the shared resource in the cell resource.

Examples

# Set the maximum shared resource size per port to 30% in the cell resource.

```
<Sysname> system-view
[Sysname] buffer egress cell shared ratio 30
```

# In an IRF, set the maximum shared resource size per port to 40% in the cell resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell shared ratio 40
```

buffer egress total-shared

Syntax

buffer egress [**slot** *slot-number*] **cell total-shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell total-shared**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone device, the *slot-number* argument can only be 1. In an IRF, with *slot-number* specified, this command configures the buffer resource of the member switch specified by *slot-number*; without *slot-number* specified, this command configures the buffer resource of all the member switches in the IRF fabric.

cell: Configures the shared resource size in the cell buffer.

ratio: Sets the shared resource size as a percentage of the cell resource or packet resource in the range of 0 to 100.

Description

Use **buffer egress total-shared** to configure the shared resource size in the cell resource or packet resource.

Use **undo buffer egress total-shared** to restore the default.

By default, on the Switch Series, 50% of the cell resource is the shared resource.

Examples

# Set 50% of the cell resource as the shared resource.

```
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

# In an IRF, set 65% of the cell resource as the shared resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell total-shared ratio 65
```

Index

Contents

AAA configuration commands

General AAA configuration commands

aaa nas-id profile

Syntax

aaa nas-id profile *profile-name*

undo aaa nas-id profile *profile-name*

View

System view

Default level

2: System level

Parameters

profile-name: Name of the NAS ID profile, a case-insensitive string of 1 to 16 characters.

Description

Use **aaa nas-id profile** to create a NAS ID profile and enter its view. A NAS ID profile maintains the bindings between NAS IDs and VLANs.

Use **undo aaa nas-id profile** to remove a NAS ID profile.

Related commands: **nas-id bind vlan**.

Examples

# Create a NAS ID profile named **aaa**.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa]
```

access-limit enable

Syntax

access-limit enable *max-user-number*

undo access-limit enable

View

ISP domain view

Default level

2: System level

Parameters

max-user-number: Maximum number of online users that the ISP domain can accommodate, in the range of 1 to 2147483646.

Description

Use **access-limit enable** to set the maximum number of online users in an ISP domain. After the number of online users reaches the allowed maximum number, no more users are accepted.

Use **undo access-limit enable** to restore the default.

By default, there is no limit to the number of online users in an ISP domain.

System resources are limited, and user connections may compete for network resources when there are many users. Setting a proper limit to the number of online users helps provide reliable system performance.

Related commands: **display domain**.

Examples

# Set a limit of 500 user connections for ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] access-limit enable 500
```

accounting command

Syntax

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting command** to specify the command line accounting method.

Use **undo accounting command** to restore the default.

By default, the default accounting method for the ISP domain is used for command line accounting.

The specified HWTACACS scheme must have been configured.

Command line accounting can use only a HWTACACS scheme.

Related commands: **accounting default** and **hwtacacs scheme**.

Examples

# Configure ISP domain **test** to use HWTACACS scheme **hwtac** for command line accounting.

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

accounting default

Syntax

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting default

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting default** to configure the default accounting method for an ISP domain.

Use **undo accounting default** to restore the default.

By default, the default accounting method of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default accounting method is used for all users who support the specified accounting method and have no specific accounting method configured.

Local accounting is only used for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure the default accounting method for ISP domain **test** to use RADIUS accounting scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting default radius-scheme rd local
```

accounting lan-access

Syntax

accounting lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }

undo accounting lan-access

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting lan-access** to configure the accounting method for LAN users.

Use **undo accounting lan-access** to restore the default.

By default, the default accounting method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **accounting default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local accounting for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access local
```

# Configure ISP domain **test** to use RADIUS accounting scheme **rd** for LAN users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

accounting login

Syntax

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting login

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting login** to configure the accounting method for login users through the console, AUX, or Asyn port or through Telnet.

Use **undo accounting login** to restore the default.

By default, the default accounting method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

Accounting is not supported for login users who use FTP.

Related commands: **local-user**, **accounting default**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local accounting for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login local
```

# Configure ISP domain **test** to use RADIUS accounting scheme **rd** for login users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login radius-scheme rd local
```

accounting optional

Syntax

accounting optional

undo accounting optional

View

ISP domain view

Default level

2: System level

Parameters

None

Description

Use **accounting optional** to enable the accounting optional feature.

Use **undo accounting optional** to disable the feature.

By default, the feature is disabled.

After you configure the **accounting optional** command for a domain, a user who would otherwise be disconnected can continue to use the network resources when no accounting server is available or when communication with the current accounting server fails. However, the switch no longer sends real-time accounting updates for the user. The accounting optional feature applies to scenarios where accounting is not important.

After you configure the **accounting optional** command, the setting configured by the **access-limit** command in local user view is not effective.

Examples

# Enable the accounting optional feature for users in domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting optional
```

accounting portal

Syntax

accounting portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting portal** to configure the accounting method for portal users.

Use **undo accounting portal** to restore the default.

By default, the default accounting method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **accounting default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local accounting for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal local
```

# Configure ISP domain **test** to use RADIUS scheme **rd** for accounting on portal users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal radius-scheme rd local
```

authentication default

Syntax

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication default

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication default** to configure the default authentication method for an ISP domain.

Use **undo authentication default** to restore the default.

By default, the default authentication method of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default authentication method is used for all users who support the specified authentication method and have no specific authentication method configured.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure the default authentication method for ISP domain **test** to use RADIUS authentication scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

authentication lan-access

Syntax

authentication lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }

undo authentication lan-access

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication lan-access** to configure the authentication method for LAN users.

Use **undo authentication lan-access** to restore the default.

By default, the default authentication method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **authentication default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authentication for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access local
```

# Configure ISP domain **test** to use RADIUS authentication scheme **rd** for LAN users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

authentication login

Syntax

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication login

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication login** to configure the authentication method for login users through the console, AUX, or Asyn port, Telnet, or FTP.

Use **undo authentication login** to restore the default.

By default, the default authentication method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

Related commands: **local-user**, **authentication default**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authentication for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
```

# Configure ISP domain **test** to use RADIUS authentication scheme **rd** for login users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```

authentication portal

Syntax

authentication portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication portal** to configure the authentication method for portal users.

Use **undo authentication portal** to restore the default.

By default, the default authentication method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **authentication default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authentication for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal local
```

# Configure ISP domain **test** to use RADIUS scheme **rd** for authentication of portal users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal radius-scheme rd local
```

authentication super

Syntax

authentication super { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* }

undo authentication super

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication super** to configure the authentication method for user privilege level switching.

Use **undo authentication super** to restore the default.

By default, the default authentication method for the ISP domain is used for user privilege level switching authentication.

The specified RADIUS or HWTACACS authentication scheme must have been configured.

Related commands: **hwtacacs scheme** and **radius scheme**; **super authentication-mode** (*Fundamentals Command Reference*).

Examples

# Configure ISP domain **test** to use HWTACACS scheme **tac** for user privilege level switching authentication.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
[Sysname] domain test
[Sysname-domain-test] authentication super hwtacacs-scheme tac
```

authorization command

Syntax

authorization command { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** | **none**] | **local** | **none** }

undo authorization command

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated user can access only commands of Level 0.

Description

Use **authorization command** to configure the command line authorization method.

Use **undo authorization command** to restore the default.

By default, the default authorization method for the ISP domain is used for command line authorization.

The specified HWTACACS scheme must have been configured.

With command line authorization configured, a user who has logged in to the switch can execute only the commands with a level lower than or equal to that of the local user.

Related commands: **local-user**, **authorization default**, and **hwtacacs scheme**.

Examples

# Configure ISP domain **test** to use local command line authorization.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command local
```

# Configure ISP domain **test** to use HWTACACS scheme **hwtac** for command line authorization and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

authorization default

Syntax

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization default

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. After passing authentication, non-login users can access the network, FTP users can access the root directory of the switch, and other login users can access only the commands of Level 0.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization default** to configure the default authorization method for an ISP domain.

Use **undo authorization default** to restore the default.

By default, the default authorization method for the ISP domain of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default authorization method is used for all users who support the specified authorization method and have no specific authorization method are configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure the default authorization method for ISP domain **test** to use RADIUS authorization scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization default radius-scheme rd local
```

authorization lan-access

Syntax

authorization lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }

undo authorization lan-access

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated LAN user can access the network directly.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization lan-access** to configure the authorization method for LAN users.

Use **undo authorization lan-access** to restore the default.

By default, the default authorization method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authorization for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access local
```

# Configure ISP domain **test** to use RADIUS authorization scheme **rd** for LAN users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access radius-scheme rd local
```

authorization login

Syntax

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization login

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. After passing authentication, FTP users can access the root directory of the switch, and other login users can access only the commands of Level 0.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization login** to configure the authorization method for login users through the console, AUX, or Asyn port, Telnet, or FTP.

Use **undo authorization login** to restore the default.

By default, the default authorization method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, **hwtacacs scheme**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authorization for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

# Configure ISP domain **test** to use RADIUS authorization scheme **rd** for login users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

authorization portal

Syntax

authorization portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated portal user can access the network directly.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization portal** to configure the authorization method for portal users.

Use **undo authorization portal** to restore the default.

By default, the default authorization method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, and **radius scheme**.

Examples

# Configure ISP domain **test** to use local authorization for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal local
```

# Configure ISP domain **test** to use RADIUS scheme **rd** for authorization of portal users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal radius-scheme rd local
```

authorization-attribute user-profile

Syntax

authorization-attribute user-profile *profile-name*

undo authorization-attribute user-profile

View

ISP domain view

Default level

3: Manage level

Parameters

profile-name: Name of the user profile, a case-sensitive string of 1 to 31 characters. For more information about user profile configuration, see *Security Configuration Guide*.

Description

Use **authorization-attribute user-profile** to specify the default authorization user profile for an ISP domain.

Use **undo authorization-attribute user-profile** to restore the default.

By default, an ISP domain has no default authorization user profile.

After a user of an ISP domain passes authentication, if the server (or the switch in the case of local authentication) does not authorize any user profile to the ISP domain, the system uses the user profile specified by the **authorization-attribute user-profile** command as that of the ISP domain.

If you configure the **authorization-attribute user-profile** command repeatedly, only the last one takes effect.

Examples

# Specify the default authorization user profile for domain **test** as **profile1**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute user-profile profile1
```

cut connection

Syntax

cut connection { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]

View

System view

Default level

2: System level

Parameters

access-type: Specifies the user connections of the specified access type.

- **dot1x**: Indicates 802.1X authentication.
- **mac-authentication**: Indicates MAC address authentication.
- **portal**: Indicates portal authentication.

all: Specifies all user connections.

domain *isp-name*: Specifies the user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies the user connections on an interface. Only Layer 2 Ethernet interfaces are supported.

ip *ip-address*: Specifies the user connections for an IP address.

mac *mac-address*: Specifies the user connections for a MAC address, with *mac-address* in the format H-H-H.

ucibindex *ucib-index*: Specifies the user connection that uses the connection index. The *ucib-index* argument ranges from 0 to 4294967295.

user-name *user-name*: Specifies the user connections that use the username. The *user-name* argument is a case-sensitive string of 1 to 80 characters. For a username entered without a domain name, the system assumes that the user is in the default domain or the mandatory authentication domain.

vlan *vlan-id*: Specifies the user connections of a VLAN, with *vlan-id* ranging from 1 to 4094.

slot *slot-number*: Specifies the user connections on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **cut connection** to tear down user connections forcibly.

This command applies to only LAN access and portal.

For 802.1X users whose usernames carry the version number or contain spaces, you cannot cut the connections by username.

For 802.1X users whose usernames use a slash (/) or backslash (\) as the domain name delimiter, you cannot cut their connections by username. For example, the **cut connection user-name aaa\bbb** command cannot cut the connections of the user **aaa\bbb**.

An interface that is configured with a mandatory authentication domain treats users of the corresponding access type as users in the mandatory authentication domain. For example, if you configure an 802.1X mandatory authentication domain on an interface, the interface uses the domain's AAA methods for all its 802.1X users. To cut connections of such users, use the **cut connection domain** *isp-name* command and specify the mandatory authentication domain.

Related commands: **display connection** and **service-type**.

Examples

# Tear down all connections of ISP domain **test.**

```
<Sysname> system-view
[Sysname] cut connection domain test
```

display connection

Syntax

display connection [**access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

access-type: Specifies the user connections of the specified access type.

- **dot1x**: Indicates 802.1X authentication.
- **mac-authentication**: Indicates MAC address authentication.
- **portal**: Indicates portal authentication.

domain *isp-name*: Specifies the user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies the user connections on an interface. Only Layer 2 Ethernet interfaces are supported.

ip *ip-address*: Specifies the user connections of an IP address.

mac *mac-address*: Specifies the user connections of a MAC address, with *mac-address* in the format H-H-H.

ucibindex *ucib-index*: Specifies the user connection that uses the connection index. The value range is from 0 to 4294967295.

user-name *user-name*: Specifies the user connections that use the username. The *user-name* argument is a case-sensitive string of 1 to 80 characters. For a username entered without a domain name, the system assumes that the user is in the default domain name or the mandatory authentication domain.

vlan *vlan-id*: Specifies the user connections of a VLAN, with *vlan-id* ranging from 1 to 4094.

slot *slot-number*: Specifies the user connections on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display connection** to display information about AAA user connections.

This command does not display information about FTP user connections.

With no parameter specified, this command displays brief information about all AAA user connections.

If you specify the **ucibindex** *ucib-index* option, this command displays detailed information. Otherwise, this command displays brief information.

If an interface is configured with a mandatory authentication domain (for example, an 802.1X mandatory authentication domain), the switch uses the mandatory authentication domain to perform authentication, authorization, and accounting for users who access the interface through the specified access type. To display connections of such users, use the **display connection domain** *isp-name* command and specify the mandatory authentication domain.

How the switch displays the username of a user on an interface configured with a mandatory authentication domain depends on the format of the username entered by the user at login:

- If the username does not contain the character @, the switch displays the username in the format *username @mandatory authentication domain name*.
- If the username contains the character @, the switch displays the entered username. For example, if a user entered the username **aaa@123** at login and the name of the mandatory authentication domain is **dom**, the switch displays the username **aaa@123**, rather than **aaa@123@dom**.

For 802.1X users whose usernames use a slash (/) or backslash (\) as the domain name delimiter, you cannot query the connections by username. For example, the **display connection user-name aaa\bbb** command cannot display the connections of the user **aaa\bbb**.

Related commands: **cut connection**.

Examples

#Display information about all AAA user connections.

```
<Sysname> display connection
Slot:  1
Index=0   , Username=telnet@system
IP=10.0.0.1
IPv6=N/A

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

# Display information about AAA user connections using the index of 0.

```
<Sysname> display connection ucibindex 0
Slot:  1
Index=0   , Username=telnet@system
IP=10.0.0.1
```

```
IPv6=N/A
Access=Admin   ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
Initial VLAN=999, Authorized VLAN=20
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2011-01-16 10:53:03 ,Current=2011-01-16 10:57:06 ,Online=00h04m03s
 Total 1 connection matched.
Slot:  2
 Total 0 connection matched.
```

Table 1 Command output

Field	Description
Slot	Slot number of the card.
Username	Username of the connection, in the format *username@domain*.
MAC	MAC address of the user.
IP	IPv4 address of the user.
IPv6	IPv6 address of the user.
Access	User access type.
ACL Group	Authorization ACL group. If no authorization ACL group is assigned, this field displays **Disable**.
User Profile	Authorization user profile.
CAR(kbps)	Authorized CAR parameters.
UpPeakRate	Uplink peak rate.
DnPeakRate	Downlink peak rate.
UpAverageRate	Uplink average rate.
DnAverageRate	Downlink average rate.

display domain

Syntax

display domain [*isp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

isp-name: Name of an existing ISP domain, a string of 1 to 24 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display domain** to display the configuration of ISP domains.

If you do not specify any ISP domain, the command displays the configuration of all ISP domains.

Related commands: **access-limit enable**, **domain**, and **state**.

Examples

# Display the configuration of all ISP domains.

```
<Sysname> display domain
0  Domain : system
   State :  Active
   Access-limit :  Disabled
   Accounting method : Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes :

1  Domain : test
   State : Active
   Access-limit : Disabled
   Accounting method : Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Lan-access authentication scheme   : radius:test, local
   Lan-access authorization scheme    : hwtacacs:hw, local
   Lan-access accounting scheme       : local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes :
    User-profile : profile1

Default Domain Name: system
Total 2 domain(s).
```

Table 2 Command output

Field	Description
Domain	ISP domain name.
State	Status of the ISP domain: active or blocked. Users in an active ISP domain can request network services, and users in a blocked ISP domain cannot.
Access-limit	Limit on the number of user connections. If there is no limit on the number, this field displays **Disabled**.
Accounting method	Indicates whether accounting is required. If accounting is required, when no accounting server is available or communication with the accounting server fails, user connections are torn down. Otherwise, users can continue to use network services.
Default authentication scheme	Default authentication method.
Default authorization scheme	Default authorization method.
Default accounting scheme	Default accounting method.
Lan-access authentication scheme	Authentication method for LAN users.
Lan-access authorization scheme	Authorization method for LAN users.
Lan-access accounting scheme	Accounting method for LAN users.
Domain User Template	Indicates some functions and attributes set for users in the domain.
Idle-cut	Indicates whether the idle cut function is enabled. With the idle cut function enabled for a domain, the system logs out any user in the domain whose traffic is less than the specified minimum traffic during the idle timeout period.
Self-service	Indicates whether the self service function is enabled. With the self service function enabled, users can launch a browser and enter the self service URL in the address bar to access the self service pages and perform self service operations.
Authorization attributes	Default authorization attributes for the ISP domain.
User-profile	Default authorization user profile.

domain

Syntax

domain *isp-name*

undo domain *isp-name*

View

System view

Default level

3: Manage level

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain slash (/), backslash (\), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), quotation marks ("), vertical bar (|), or at sign (@).

Description

Use **domain** *isp-name* to create an ISP domain and enter ISP domain view.

Use **undo domain** to remove an ISP domain.

By default, there is a system predefined ISP domain named **system** in the system.

All ISP domains are in active state when they are created.

You cannot delete the system predefined ISP domain **system**, and can only modify its configuration.

To delete the ISP domain that is used as the default ISP domain, you must change it to a non-default ISP domain first by using the **undo domain default enable** command.

Related commands: **state** and **display domain**.

Examples

# Create ISP domain **test**, and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

View

System view

Default level

3: Manage level

Parameters

isp-name: Name of the ISP domain, a case-insensitive string of 1 to 24 characters.

Description

Use **domain default enable** to specify the default ISP domain. Users without any domain name carried in the usernames are considered to be in the default domain.

Use **undo domain default enable** to restore the default.

By default, the default ISP domain is the system predefined ISP domain **system**.

There can be only one default ISP domain.

The specified domain must already exist. Otherwise, users without any domain name carried in the username cannot pass authentication.

To delete the ISP domain that is used as the default ISP domain, you must change it to a non-default ISP domain first by using the **domain default disable** command.

Related commands: **domain**, **state**, and **display domain**.

Examples

# Create a new ISP domain named **test**, and configure it as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] quit
[Sysname] domain default enable test
```

idle-cut enable

Syntax

idle-cut enable *minute* [*flow*]

undo idle-cut enable

View

ISP domain view

Default level

2: System level

Parameters

minute: Idle timeout period, in the range of 1 to 600 minutes.

flow: Minimum traffic during the idle timeout period, which is in the range of 1 to 10240000 bytes and defaults to 10240.

Description

Use **idle-cut enable** to enable the idle cut function and set the relevant parameters. With the idle cut function enabled for a domain, the switch checks the traffic of each online user in the domain at the idle timeout interval, and logs out any user in the domain whose traffic during the idle timeout period is less than the specified minimum traffic.

Use **undo idle-cut enable** to restore the default.

By default, the function is disabled.

You can also set the idle timeout period on the server to make the server log out users whose traffic during the idle timeout period is less than 10240 bytes, but your setting on the server takes effect only when you disable the idle cut function on the switch.

Related commands: **domain**.

Examples

# Enable the idle cut function and set the idle timeout period to 50 minutes and the traffic threshold to 1024 bytes for ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] idle-cut enable 50 1024
```

nas-id bind vlan

Syntax

nas-id *nas-identifier* **bind vlan** *vlan-id*

undo nas-id *nas-identifier* **bind vlan** *vlan-id*

View

NAS ID profile view

Default level

2: System level

Parameters

nas-identifier: NAS ID, a case-sensitive string of 1 to 20 characters

vlan-id: ID of the VLAN to be bound with the NAS ID, in the range of 1 to 4094.

Description

Use **nas-id bind vlan** to bind a NAS ID with a VLAN.

Use **undo nas-id bind vlan** to remove a NAS ID-VLAN binding.

By default, no NAS ID-VLAN binding exists.

In a NAS ID profile view, you can configure multiple NAS ID–VLAN bindings.

A NAS ID can be bound with more than one VLAN, but one VLAN can be bound with only one NAS ID. If you bind a VLAN with different NAS IDs, only the last binding takes effect.

Related commands: **aaa nas-id profile**.

Examples

# Bind NAS ID 222 with VLAN 2.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

self-service-url enable

Syntax

self-service-url enable *url-string*

undo self-service-url enable

View

ISP domain view

Default level

2: System level

Parameters

url-string: URL of the self-service server, a string of 1 to 64 characters. It must start with http:// and contain no question mark. This URL was specified by the RADIUS server administrator during RADIUS server installation.

Description

Use **self-service-url enable** to enable the self-service server location function and specify the URL of the self-service server.

Use **undo self-service-url enable** to restore the default.

By default, the self-service server location function is disabled.

With the self-service function, users can manage and control their accounts and passwords. Only the RADIUS server systems provided by Intelligent Management Center (IMC) support the self-service function.

Examples

# For ISP domain **test**, enable the self-service server location function and specify the URL of the self-service server for changing user password to http://10.153.89.94/selfservice.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] self-service-url enable http://10.153.89.94/selfservice
```

state (ISP domain view)

Syntax

state { **active** | **block** }

undo state

View

ISP domain view

Default level

2: System level

Parameters

active: Places the ISP domain in active state to allow the users in the ISP domain to request network services.

block: Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.

Description

Use **state** to set the status of an ISP domain.

Use **undo state** to restore the default.

By default, an ISP domain is in active state.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. The online users are not affected.

Examples

# Place the current ISP domain **test** to the state of blocked.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

Local user configuration commands

access-limit

Syntax

access-limit *max-user-number*

undo access-limit

View

Local user view

Default level

3: Manage level

Parameters

max-user-number: Maximum number of concurrent users of the current local user account, in the range of 1 to 1024.

Description

Use **access-limit** to limit the number of concurrent users of a local user account.

Use **undo access-limit** to remove the limitation.

By default, there is no limit to the number of users who concurrently use the same local user account.

This command takes effect only when local accounting is used for the user account.

This limit is not effective for FTP users because accounting is not available for FTP users.

Related commands: **display local-user**.

Examples

# Limit the maximum number of concurrent users of local user account **abc** to 5.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] access-limit 5
```

authorization-attribute (local user view/user group view)

Syntax

authorization-attribute { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **user-role** { **guest** | **guest-manager** | **security-audit** } | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **callback-number** | **idle-cut** | **level** | **user-profile** | **user-role** | **vlan** | **work-directory** } *

View

Local user view, user group view

Default level

3: Manage level

Parameters

acl *acl-number*: Specifies the authorization ACL. The ACL number must be in the range of 2000 to 5999. After passing authentication, a local user is authorized to access the network resources specified by this ACL.

callback-number *callback-number*: Specifies the authorized PPP callback number. The *callback-number* argument is a case-sensitive string of 1 to 64 characters. After a local user passes authentication, the switch uses this number to call the user.

idle-cut *minute*: Sets the idle timeout period. With the idle cut function enabled, an online user whose idle period exceeds the specified idle timeout period is logged out. The *minute* argument indicates the idle timeout period, in the range of 1 to 120 minutes.

level *level*: Specifies the user level, which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower level. If the user interfaces' authentication mode is **scheme**, which commands users can use after login in depends on this argument. By default, the user level is 0, and users can use only commands of level 0 after login.

user-profile *profile-name*: Specifies the authorization user profile. *profile-name* is a case-sensitive string of 1 to 32 characters. It can contain letters, digits, and underscores (_) and must start with a letter. After a user passes authentication and gets online, the switch uses the settings in the user profile to restrict the access behavior of the user. For more information about user profiles, see *Security Configuration Guide*.

user-role: Specifies the role for the local user. This keyword is available in only local user view. Users playing different roles can access different levels of commands. If you specify no role for a local user, the access right of the user after login depends on other authorization attributes. Supported roles include:

- **guest**: A guest user account is usually created through the Web interface.
- **guest-manager**: After passing authentication, a guest manager can only use the Web interface to access guest-related pages to, for example, create, modify, or change guest user accounts.
- **security-audit**: A local user playing this role is a security log administrator After passing authentication, a security log administrator can manage security log files, for example, save security log files. For more information about the commands that a security log administrator can use, see *Network Management and Monitoring Command Reference.*

vlan *vlan-id*: Specifies the authorized VLAN. The *vlan-id* argument is in the range of 1 to 4094. After passing authentication, a local user can access the resources in this VLAN.

work-directory *directory-name*: Specifies the work directory, if the user or users use the FTP or SFTP service. The *directory-name* argument is a case-insensitive string of 1 to 135 characters. The directory must already exist. By default, an FTP or SFTP user can access the root directory of the switch.

Description

Use **authorization-attribute** to configure authorization attributes for the local user or user group. After the local user or a local user of the user group passes authentication, the switch assigns these attributes to the user.

Use **undo authorization-attribute** to remove authorization attributes and restore the defaults.

By default, no authorization attribute is configured for a local user or user group.

Every configurable authorization attribute has its definite application environments and purposes. Consider the service types of users when assigning authorization attributes.

Authorization attributes configured for a user group are effective for all local users in the group. You can group local users to improve configuration and management efficiency.

An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view. If an authorization attribute is configured in user group view but not in local user view, the setting in user group view takes effect.

To make sure that FTP and SFTP users can access the directory after a switchover between the main card and the backup card, do not specify slot information for the work directory.

If only one user is playing the role of security log administrator in the system, you cannot delete the user account, or remove or change the user's role, unless you configure another user as a security log administrator first.

A local user can play only one role at a moment. If you perform the role configuration repeatedly, only the last role configuration takes effect.

Examples

# Configure the authorized VLAN of local user **abc** as VLAN 2.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] authorization-attribute vlan 2
```

# Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

bind-attribute

Syntax

bind-attribute { **call-number** *call-number* [**:** *subcall-number*] | **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **call-number** | **ip** | **location** | **mac** | **vlan** } *

View

Local user view

Default level

3: Manage level

Parameters

call-number *call-number*: Specifies a calling number for ISDN user authentication. The *call-number* argument is a string of 1 to 64 characters. This option applies only to PPP users.

subcall-number: Specifies the sub-calling number. The total length of the calling number and the sub-calling number cannot be more than 62 characters.

ip *ip-address*: Specifies the IP address of the user. This option applies only to 802.1X users.

location port *slot-number subslot-number port-number*: Specifies the port to which the user is bound, where *slot-number* is in the range of 0 to 255, *subslot-number* is in the range of 0 to 15, and *port-number* is in the range of 0 to 255. This option applies only to LAN users.

mac *mac-address*: Specifies the MAC address of the user in the format H-H-H. This option applies only to LAN users.

vlan *vlan-id*: Specifies the VLAN to which the user belongs, where *vlan-id* is in the range of 1 to 4094. This option applies only to LAN users.

Description

Use **bind-attribute** to configure binding attributes for a local user.

Use **undo bind-attribute** to remove binding attributes of a local user.

By default, no binding attribute is configured for a local user.

Binding attributes are checked upon authentication of a local user. If the binding attributes of a local user do not match the configured ones, the user fails the checking and the authentication.

Binding attribute checking does not take the service types of the users into account. A configured binding attribute is effective for all types of users. Be cautious when deciding which binding attributes should be configured for which type of local users. For example, an IP address binding applies only to 802.1X authentication that supports IP address upload. If you configure an IP address binding for an authentication method that does not support IP address upload, for example, MAC authentication, the local authentication fails.

Examples

# Configure the bound IP of local user **abc** as 3.3.3.3.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] bind-attribute ip 3.3.3.3
```

display local-user

Syntax

display local-user [**idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** | **web** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

idle-cut { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

service-type: Specifies the local users who use a specific type of service.

- **ftp**: FTP users.
- **lan-access**: Users accessing the network through Ethernet, such as 802.1X users.
- **portal**: Portal users.
- **ssh**: SSH users.
- **telnet**: Telnet users.
- **terminal**: Users logging in through the console or AUX port.
- **web**: Web users.

state { **active** | **block** }: Specifies local users in the state of active or blocked. A local user in active state can access network services, but a local user in blocked state cannot.

user-name *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters and does not contain the domain name.

vlan *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies the local users on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display local-user** to display configuration and statistics information about local users.

If you do not specify any parameter, the command displays information about all local users.

Related commands: **local-user**.

Examples

# Display information about all local users.

```
<Sysname> display local-user
The contents of local user abc:
 State:                     Active
 ServiceType:               lan-access
 Access-limit:              Enabled          Current AccessNum: 0
 Max AccessNum:             300
 User-group:                system
 Bind attributes:
  IP address:               1.2.3.4
  Bind location:            1/4/1 (SLOT/SUBSLOT/PORT)
  MAC address:              0001-0002-0003
  Vlan ID:                  100
 Authorization attributes:
  Idle TimeOut:             10(min)
  Work Directory:           flash:/
  User Privilege:           3
  Acl ID:                   2000
  Vlan ID:                  100
  User Profile:             prof1
 Expiration date:           12:12:12-2018/09/16
 Password aging:            Enabled (30 days)
 Password length:           Enabled (4 characters)
 Password composition:      Enabled (4 types,  2 characters per type)
Total 1 local user(s) matched.
```

Table 3 Command output

Field	Description
State	Status of the local user: active or blocked.
ServiceType	Service types that the local user can use, including FTP, LAN, portal, SSH, Telnet, terminal, and web.
Access-limit	Whether or not to limit the number of concurrent connections of the username.
Current AccessNum	Number of connections that currently use the username.
Max AccessNum	Maximum number of concurrent connections of the username.
Bind attributes	Binding attributes of the local user.
VLAN ID	VLAN to which the user is bound.
Calling Number	Calling number bound for the ISDN user.
Authorization attributes	Authorization attributes of the local user.
Idle TimeOut	Idle timeout period of the user, in minutes.
Callback-number	Authorized PPP callback number of the local user.
Work Directory	Directory that the FTP user can access.
VLAN ID	Authorized VLAN of the local user.
User Profile	User profile for local user authorization.
Expiration date	Expiration time of the local user.
Password aging	Aging time of the local user password.
Password length	Minimum length of the local user password.
Password composition	Password composition policy of the local user.

display user-group

Syntax

display user-group [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display user-group** to display user group configuration. If you do not specify any user group name, the command displays information about all users groups.

Related commands: **user-group**.

Examples

# Display the configuration of user group **abc**.

```
<Sysname> display user-group abc
The contents of user group abc:
 Authorization attributes:
  Idle-cut:                120(min)
  Work Directory:          FLASH:
  Level:                   1
  Acl Number:              2000
  Vlan ID:                 1
  User-Profile:            1
  Callback-number:         1
 Password aging:           Enabled (1 days)
 Password length:          Enabled (4 characters)
 Password composition:     Enabled (1 types,  1 characters per type)
Total 1 user group(s) matched.
```

Table 4 Command output

Field	Description
Idle-cut	Idle timeout interval, in minutes.
Work Directory	Directory that FTP/SFTP users in the group can access.
Level	Local user level.
ACL Number	Authorization ACL.
VLAN ID	Authorized VLAN.
Callback-number	Authorized PPP callback number.
Password aging	Aging time of the local user password.
Password length	Minimum length of the local user password.
Password composition	Password composition policy of the local user.

expiration-date (local user view)

Syntax

expiration-date *time*

undo expiration-date

View

Local user view

Default level

3: Manage level

Parameters

time: Expiration time of the local user, in the format HH:MM:SS-MM/DD/YYYY, HH:MM:SS-YYYY/MM/DD, MM/DD/YYYY-HH:MM:SS, or YYYY/MM/DD-HH:MM:SS. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. MM/DD/YYYY or YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **expiration-date** to set the expiration time of a local user.

Use **undo expiration-date** to remove the configuration.

By default, a local user has no expiration time and no time validity checking is performed.

For temporary network access requirements, create a guest account and specify a validity time and an expiration time for the account to control the validity of the account. When a user uses the guest account for local authentication and passes the authentication, the switch checks whether the current system time is between the validity time and the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Related commands: **validity-date**.

Examples

# Set the expiration time of user **abc** to 12:10:20 on Jan 31, 2011.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2011/01/31
```

group

Syntax

group *group-name*

undo group

View

Local user view

Default level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use **group** to assign a local user to a user group.

Use **undo group** to restore the default.

By default, a local user belongs to the system default user group **system**.

Examples

# Assign local user 111 to user group **abc**.

```
<Sysname> system-view
[Sysname] local-user 111
[Sysname-luser-111] group abc
```

group-attribute allow-guest

Syntax

group-attribute allow-guest

undo group-attribute allow-guest

View

User group view

Default level

3: Manage level

Parameters

None

Description

Use **group-attribute allow-guest** to set the guest attribute for a user group so that guest users created by a guest manager through the Web interface can join the group.

Use **undo group-attribute allow-guest** to restore the default.

By default, the guest attribute is not set for a user group, and guest users created by a guest manager through the Web interface cannot join the group.

The guest attribute is set for the system predefined user group **system** by default, and you cannot remove the attribute for the user group.

Examples

# Set the guest attribute for user group **test**.

```
<Sysname> system-view
[Sysname] user-group test
[Sysname-ugroup-test] group-attribute allow-guest
```

local-user

Syntax

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** | **web** }] }

View

System view

Default level

3: Manage level

Parameters

user-name: Name for the local user, a case-sensitive string of 1 to 55 characters that does not contain the domain name. It cannot contain slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.

all: Specifies all users.

service-type: Specifies the users of a type.

- **ftp**: FTP users.
- **lan-access**: Users accessing the network through an Ethernet, such as 802.1X users.
- **portal**: Portal users.
- **ssh**: SSH users.
- **telnet**: Telnet users.
- **terminal**: Users logging in through the console or AUX port.
- **web**: Web users.

Description

Use **local-user** to add a local user and enter local user view.

Use **undo local-user** to remove the specified local users.

By default, no local user is configured.

Related commands: **display local-user** and **service-type**.

Examples

# Add a local user named **user1**.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

password (local user view)

Syntax

password [{ **cipher** | **simple** } *password*]

undo password

View

Local user view

Default level

2: System level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

Description

Use **password** to configure a password for a local user.

Use **undo password** to delete the password of a local user.

If none of the parameters is specified, you enter the interactive mode to set a plaintext password. The interactive mode is supported only on switches that support the password control feature. For more information about password control commands, see *Security Command Reference*.

When the password control feature is globally enabled by using the **password-control enable** command, local user passwords, such as the length and complexity, are under the restriction of the password control feature, and are not displayed.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Related commands: **display local-user**.

Examples

# Set the password of local user **user1** to 123456 in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456
```

# Set the password of local user **user1** to 123456 in interactive mode.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password
Password:******
Confirm :******
```

service-type

Syntax

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * | **portal** | **web** }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * | **portal** | **web** }

View

Local user view

Default level

3: Manage level

Parameters

ftp: Authorizes the user to use the FTP service. The user can use the root directory of the FTP server by default.

lan-access: Authorizes the user to use the LAN access service. Such users are mainly Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service, allowing the user to log in through the console or AUX port.

portal: Authorizes the user to use the Portal service.

web: Authorizes the user to use the Web service.

Description

Use **service-type** to specify the service types that a user can use.

Use **undo service-type** to delete service types configured for a user.

By default, a user is authorized with no service.

You can execute the **service-type** command repeatedly to specify multiple service types for a user.

Examples

# Authorize user **user1** to use the Telnet service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

state (local user view)

Syntax

state { **active** | **block** }

undo state

View

Local user view

Default level

2: System level

Parameters

active: Places the local user in active state to allow the local user to request network services.

block: Places the local user in blocked state to prevent the local user from requesting network services.

Description

Use **state** to set the status of a local user.

Use **undo state** to restore the default.

By default, a local user is in active state.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related commands: **local-user**.

Examples

# Place local user **user1** to the blocked state.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] state block
```

user-group

Syntax

user-group *group-name*

undo user-group *group-name*

View

System view

Default level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use **user-group** to create a user group and enter its view.

Use **undo user-group** to remove a user group.

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. Configurable user attributes include password control attributes and authorization attributes.

A user group with one or more local users cannot be removed.

The system predefined user group **system** cannot be removed, but you can change its configurations.

Related commands: **display user-group**.

Examples

# Create a user group named **abc** and enter its view.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

validity-date

Syntax

validity-date *time*

undo validity-date

View

Local user view

Default level

3: Manage level

Parameters

time: Validity time of the local user, in the format HH:MM:SS-MM/DD/YYYY, HH:MM:SS-YYYY/MM/DD, MM/DD/YYYY-HH:MM:SS, or YYYY/MM/DD-HH:MM:SS. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. MM/DD/YYYY or YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **validity-date** to set the validity time of a local user.

Use **undo validity-date** to remove the configuration.

By default, a local user has no validity time and no time validity checking is performed.

For temporary network access requirements, create a guest account and specify a validity time and an expiration time for the account to control the validity of the account. When a user uses the guest account for local authentication and passes the authentication, the switch checks whether the current system time is between the validity time and the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Related command: **expiration-date**.

Examples

# Set the validity time of user **abc** to 12:10:20 on April 30, 2011, and the expiration time to 12:10:20 on May 31, 2011.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] validity-date 12:10:20-2011/04/30
[Sysname-luser-abc] expiration-date 12:10:20-2011/05/31
```

RADIUS configuration commands

accounting-on enable

Syntax

accounting-on enable [**interval** *seconds* | **send** *send-times*] *

undo accounting-on enable

View

RADIUS scheme view

Default level

2: System level

Parameters

seconds: Time interval for retransmitting an accounting-on packet in seconds, ranging from 1 to 15. The default setting is 3 seconds.

send-times: Maximum number of accounting-on packet transmission attempts, ranging from 1 to 255. The default setting is 50.

Description

Use **accounting-on enable** to configure the accounting-on feature. This feature enables the switch to, after rebooting, automatically send an accounting-on message to the RADIUS accounting server indicated by the RADIUS scheme to stop accounting for and log out online users.

Use **undo accounting-on enable** to disable the accounting-on feature.

By default, the accounting-on feature is disabled.

Parameters set with the **accounting-on enable** command take effect immediately.

After executing the **accounting-on enable** command, issue the **save** command to make sure that the command takes effect after the switch reboots. For information about the **save** command, see *Fundamentals Command Reference*.

Related commands: **radius scheme**.

Examples

# Enable the accounting-on feature for RADIUS authentication scheme **radius1**, set the retransmission interval to 5 seconds, and set the transmission attempts to 15.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

attribute 25 car

Syntax

attribute 25 car

undo attribute 25 car

View

RADIUS scheme view

Default level

2: System level

Parameters

None

Description

Use **attribute 25 car** to specify to interpret the RADIUS class attribute (attribute 25) as CAR parameters.

Use **undo attribute 25 car** to restore the default.

By default, RADIUS attribute 25 is not interpreted as CAR parameters.

Related commands: **display radius scheme** and **display connection**.

Examples

# Specify to interpret RADIUS attribute 25 as CAR parameters.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 25 car
```

data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

View

RADIUS scheme view

Default level

2: System level

Parameters

data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use **data-flow-format** to set the traffic statistics unit for data flows or packets.

Use **undo data-flow-format** to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

The unit for data flows and that for packets must be consistent with those on the RADIUS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display radius scheme**.

Examples

# Set the traffic statistics unit for data flows and that for packets to kilobytes and kilo-packets respectively in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display radius scheme

Syntax

display radius scheme [*radius-scheme-name*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

radius-scheme-name: RADIUS scheme name.

slot *slot-number*: Specifies the RADIUS schemes on an IRF member device. The *slot-number* argument represents the ID of an IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display radius scheme** to display the configuration of RADIUS schemes.

If you do not specify any RADIUS scheme, the command displays the configuration of all RADIUS schemes.

Related commands: **radius scheme**.

Examples

# Display the configuration of all RADIUS schemes.

```
<Sysname> display radius scheme
------------------------------------------------------------------
SchemeName  : radius1
  Index : 0                           Type : extended
  Primary Auth Server:
    IP: 1.1.1.1                                  Port: 1812   State: active
    Encryption Key : ******
    Probe username : test
    Probe interval : 60 min
  Primary Acct Server:
    IP: 1.1.1.1                                  Port: 1813   State: active
    Encryption Key : ******
  Second Auth Server:
    IP: 1.1.2.1                                  Port: 1812   State: active
    Encryption Key : N/A
    Probe username : test
    Probe interval : 60 min
    IP: 1.1.3.1                                  Port: 1812   State: active
    Encryption Key : N/A
    Probe username : test
    Probe interval : 60 min
  Second Acct Server:
    IP: 1.1.2.1                                  Port: 1813   State: block
    Encryption Key : N/A
  Auth Server Encryption Key : ******
  Acct Server Encryption Key : N/A
  Accounting-On packet disable, send times : 50 , interval : 3s
  Interval for timeout(second)                            : 3
  Retransmission times for timeout                        : 3
  Interval for realtime accounting(minute)                : 12
  Retransmission times of realtime-accounting packet      : 5
  Retransmission times of stop-accounting packet          : 500
  Quiet-interval(min)                                     : 5
  Username format                                         : without-domain
  Data flow unit                                          : Byte
  Packet unit                                             : one
  NAS-IP address                                          : 1.1.1.1
  Attribute 25                                            : car
------------------------------------------------------------------
Total 1 RADIUS scheme(s).
```

Table 5 Command output

Field	Description
SchemeName	Name of the RADIUS scheme.
Index	Index number of the RADIUS scheme.
Type	Type of the RADIUS server: extended or standard.
Primary Auth Server	Information about the primary authentication server.
Primary Acct Server	Information about the primary accounting server.
Second Auth Server	Information about the secondary authentication server.
Second Acct Server	Information about the secondary accounting server.
IP	IP address of the server.
Port	Service port of the server. If no port configuration is performed, the default port number is displayed.
State	Status of the server: active or blocked.
Encryption Key	Shared key for secure authentication or accounting communication, displayed as a series of asterisks (******). If no shared key is configured, this field displays **N/A**. This shared key is used only when no specific shared key is specified for the RADIUS server.
Probe username	Username used for server status detection.
Probe interval	Server status detection interval, in minutes.
Auth Server Encryption Key	Shared key for secure authentication communication, displayed as a series of asterisks (******). If no shared key is configured, this field displays **N/A**.
Acct Server Encryption Key	Shared key for secure accounting communication, displayed as a series of asterisks (******). If no shared key is configured, this field displays **N/A**.
Accounting-On packet disable	The accounting-on feature is disabled.
send times	Retransmission times of accounting-on packets.
interval	Interval at which the switch retransmits accounting-on packets.
Interval for timeout(second)	RADIUS server response timeout period, in seconds.
Retransmission times for timeout	Maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.
Interval for realtime accounting(minute)	Interval for real-time accounting, in minutes.
Retransmission times of realtime-accounting packet	Maximum number of accounting attempts.
Retransmission times of stop-accounting packet	Maximum number of stop-accounting attempts.
Quiet-interval(min)	Quiet interval for the primary server.
Username format	Format of the usernames to be sent to the RADIUS server.
Data flow unit	Unit for data flows sent to the RADIUS server.
Packet unit	Unit for packets sent to the RADIUS server.

Field	Description
NAS-IP address	Source IP address for RADIUS packets to be sent.
Attribute 25	Interprets RADIUS attribute 25 as the CAR parameters.

display radius statistics

Syntax

display radius statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Specifies the RADIUS packet statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display radius statistics** to display RADIUS packet statistics.

Related commands: **radius scheme**.

Examples

# Display statistics about RADIUS packets.

```
<Sysname> display radius statistics
Slot  1:state statistic(total=4096):
     DEAD = 4096      AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 0
 AcctStop = 0          OnLine = 0            Stop = 0
Received and Sent packets statistic:
Sent PKT total   = 1547     Received PKT total = 23
Resend Times     Resend total
1                508
2                508
Total            1016
RADIUS received packets statistic:
Code =  2   Num = 15       Err = 0
Code =  3   Num = 4        Err = 0
Code =  5   Num = 4        Err = 0
Code = 11   Num = 0        Err = 0
Running statistic:
RADIUS received messages statistic:
Normal auth request      Num = 24       Err = 0        Succ = 24
EAP auth request         Num = 0        Err = 0        Succ = 0
Account request          Num = 4        Err = 0        Succ = 4
Account off request      Num = 503      Err = 0        Succ = 503
PKT auth timeout         Num = 15       Err = 5        Succ = 10
PKT acct_timeout         Num = 1509     Err = 503      Succ = 1006
Realtime Account timer   Num = 0        Err = 0        Succ = 0
PKT response             Num = 23       Err = 0        Succ = 23
Accounting on response   Num = 0        Err = 0        Succ = 0
Session ctrl pkt         Num = 0        Err = 0        Succ = 0
Normal author request    Num = 0        Err = 0        Succ = 0
Set policy result        Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 10
Auth reject              Num = 14
EAP auth replying        Num = 0
Account success          Num = 4
Account failure          Num = 3
Server ctrl req          Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum  = 0
Timer_Err        = 0
Alloc_Mem_Err    = 0
State Mismatch   = 0
Other_Error      = 0
No-response-acct-stop packet = 1
Discarded No-response-acct-stop packet for buffer overflow = 0
```

Table 6 Command output

Field	Description
state statistic	User statistics, by state
DEAD	Number of idle users
AuthProc	Number of users waiting for authentication
AuthSucc	Number of users who have passed authentication
AcctStart	Number of users for whom accounting has been started
RLTSend	Number of users for whom the system sends real-time accounting packets
RLTWait	Number of users waiting for real-time accounting
AcctStop	Number of users in the state of accounting waiting stopped
OnLine	Number of online users
Stop	Number of users in the state of stop

Field	Description
Received and Sent packets statistic	Statistics for packets received and sent by the RADIUS module
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
Resend Times	Number of transmission attempts
Resend total	Number of packets retransmitted
Total	Total number of packets retransmitted
RADIUS received packets statistic	Statistics for packets received by the RADIUS module
Code	Packet type
Num	Total number of packets
Err	Number of packets that the switch failed to process
Succ	Number of messages that the switch successfully processed
Running statistic	Statistics for RADIUS messages received and sent by the RADIUS module
RADIUS received messages statistic	Statistics for received RADIUS messages
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout messages
PKT acct_timeout	Number of accounting timeout messages
Realtime Account timer	Number of real-time accounting requests
PKT response	Number of responses from servers
Accounting on response	Number of accounting-on responses
Session ctrl pkt	Number of session control messages
Normal author request	Number of normal authorization requests
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Statistics for sent RADIUS messages
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of packets for indicating timer startup failures

Field	Description
Alloc_Mem_Err	Number of packets for indication memory allocation failures
State Mismatch	Number of packets for indicating mismatching status
Other_Error	Number of packets for indicating other types of errors
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

display stop-accounting-buffer (for RADIUS)

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in a RADIUS scheme. The RADIUS scheme name is a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies the stop-accounting requests buffered for a session. The session ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies the stop-accounting requests buffered in a time range. The start time and end time must be in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD.

user-name *user-name*: Specifies the stop-accounting requests buffered for a user. The username is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

slot *slot-number*: Specifies the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stop-accounting-buffer** to display information about the stop-accounting requests buffered in the switch.

If the switch sends a stop-accounting request to a RADIUS server but receives no response, it retransmits it up to a certain number of times (defined by the **retry** command). If the switch still receives no response, it considers the stop-accounting attempt a failure, buffers the request, and makes another stop-accounting attempt. The maximum number of the stop-accounting attempts is defined by the **retry stop-accounting** command. If all attempts fail, the switch discards the request.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **user-name-format**, **retry**, and **retry stop-accounting**.

Examples

# Display information about the stop-accounting requests buffered for user **abc**.

```
<Sysname> display stop-accounting-buffer user-name abc
Slot  1:
RDIdx Session-ID               user name                  Happened time
1    1000326232325010          abc                       23:27:16-03/31/2011
1    1000326232326010          abc                       23:33:01-03/31/2011
Total 2 record(s) Matched
```

key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the shared key for secure RADIUS accounting communication.

authentication: Sets the shared key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **key** to set the shared key for secure RADIUS authentication/authorization or accounting communication.

Use **undo key** to restore the default.

By default, no shared key is configured.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

The shared keys specified during the configuration of the RADIUS servers, if any, take precedence.

The shared keys configured on the switch must match those configured on the RADIUS servers.

Related commands: **display radius scheme**.

Examples

# For RADIUS scheme **radius1**, set the shared key for secure authentication/authorization communication to **$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B** in cipher text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication cipher
$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B
```

# For RADIUS scheme **radius1**, set the shared key for secure accounting communication to **ok** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

# For RADIUS scheme **radius1**, set the shared key for secure accounting communication to **ok** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

nas-ip (RADIUS scheme view)

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: IPv4 address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address. It must be an address of the switch and must be a unicast address that is neither a loopback address nor a link-local address.

Description

Use **nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo nas-ip** to restore the default.

By default, the source IP address of an outgoing RADIUS packet is that configured by the **radius nas-ip** command in system view. If the **radius nas-ip** command is not configured, the source IP address is the IP address of the outbound interface.

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

The source IP address specified for outgoing RADIUS packets must be of the same IP version as the IP addresses of the RADIUS servers in the RADIUS scheme. Otherwise, the source IP address configuration does not take effect.

A RADIUS scheme can have only one source IP address for outgoing RADIUS packets. If you specify a new source IP address for the same RADIUS scheme, the new one overwrites the old one.

The setting configured by the **nas-ip** command in RADIUS scheme view is only for the RADIUS scheme, whereas that configured by the **radius nas-ip** command in system view is for all RADIUS schemes. The setting in RADIUS scheme view takes precedence.

Related commands: **radius nas-ip**.

Examples

# Set the source IP address for outgoing RADIUS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

primary accounting (RADIUS scheme view)

Syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key*] *

undo primary accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the primary accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server, which is a UDP port number in the range of 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the primary RADIUS accounting server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **primary accounting** to specify the primary RADIUS accounting server.

Use **undo primary accounting** to remove the configuration.

By default, no primary RADIUS accounting server is specified.

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

The IP addresses of the accounting servers and those of the authentication/authorization servers must be of the same IP version.

The IP addresses of the primary and secondary accounting servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key accounting** [**cipher** | **simple**] *key* command.

If you change the primary accounting server when the switch has already sent a start-accounting request to the server, the communication with the primary server times out, and the switch looks for a server in active state from the new primary server on.

If you remove an accounting server being used by users, the switch cannot send real-time accounting requests and stop-accounting requests anymore for the users, and does not buffer the stop-accounting requests.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **key**.

Examples

# For RADIUS scheme **radius1**, set the IP address of the primary accounting server to 10.110.1.2, the UDP port to 1813, and the shared key to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple hello
```

primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] *

undo primary authentication

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the primary authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary authentication/authorization server.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, which is a UDP port number in the range of 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the primary RADIUS authentication/authorization server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

probe username: Enables the switch to detect the status of the primary RADIUS authentication/authorization server.

username *name*: Specifies the username in the authentication request that is used to detect the status of the primary RADIUS authentication/authorization server.

interval *interval*: Specifies the interval between two server status detections. The value ranges from 1 to 3600 and defaults to 60, in minutes.

Description

Use **primary authentication** to specify the primary RADIUS authentication/authorization server.

Use **undo primary authentication** to remove the configuration.

By default, no primary RADIUS authentication/authorization server is specified.

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

The IP addresses of the authentication/authorization servers and those of the accounting servers must be of the same IP version.

The IP addresses of the primary and secondary authentication/authorization servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key authentication** [**cipher** | **simple**] *key* command.

If you remove the primary authentication server when an authentication process is in progress, the communication with the primary server times out, and the switch looks for a server in active state from the new primary server on.

With the server status detection feature enabled, the switch sends an authentication request that carries the specified username to the primary server at the specified interval. If the switch receives no response from the server within the time interval specified by the **timer response-timeout** command, the switch sends the authentication request again.

If the maximum number of retries (specified by the **retry** command) is reached and the switch still receives no response from the server, the switch considers the server as unreachable. If the switch receives a response from the server before the maximum number of retries is reached, the switch considers the server as reachable. The switch sets the status of the server to **block** or **active** according to the status detection result, regardless of the current status of the server.

For 802.1X authentication, if the status of every server is **block**, the switch assigns the port connected to an authentication user to the specified 802.1X critical VLAN. For more information about the 802.1X critical VLAN, see *Security Configuration Guide*.

To ensure that the switch can set the server to its actual status, set a longer quiet timer for the primary server with the **timer quiet** command. If you set a short quiet timer and configure 802.1X critical VLAN on a port, the switch might frequently change the server status, and the port might frequently join and leave the critical VLAN.

Related commands: **key**.

Examples

# For RADIUS scheme **radius1**, set the IP address of the primary authentication/authorization server to 10.110.1.1, the UDP port to 1812, and the shared key to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key hello
```

# In RADIUS scheme **radius1**, set the username used for status detection of the primary authentication/authorization server to **test** in plain text, and set the server status detection interval to 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 probe username test interval
120
```

radius client

Syntax

radius client enable

undo radius client

View

System view

Default level

2: System level

Parameters

None

Description

Use **radius client enable** to enable the RADIUS listening port of a RADIUS client.

Use **undo radius client** to disable the RADIUS listening port of a RADIUS client.

By default, the RADIUS listening port is enabled.

When the listening port of the RADIUS client is disabled:

- No more stop-accounting requests of online users cannot be sent out or buffered, and the RADIUS server can no longer receive logoff requests from online users. After a user goes offline, the RADIUS server still has the user's record during a certain period of time.
- The buffered accounting packets cannot be sent out and are deleted from the buffer when the configured maximum number of attempts is reached, affecting the precision of user accounting.
- If local authentication, authorization, or accounting is configured as the backup, the switch performs local authentication, authorization, or accounting instead after the RADIUS request fails. Local accounting is only for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

Examples

# Enable the listening port of the RADIUS client.

```
<Sysname> system-view
[Sysname] radius client enable
```

radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use **radius dscp** to set the DSCP value for IPv4 RADIUS protocol packets.

Use **undo radius dscp** to restore the default.

By default, the DSCP value in IPv4 RADIUS protocol packets is 0.

Examples

# Set the DSCP value to 6 for IPv4 RADIUS protocol packets.

```
<Sysname> system-view
[Sysname] radius dscp 6
```

radius ipv6 dscp

Syntax

radius ipv6 dscp *dscp-value*

undo radius ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use **radius ipv6 dscp** to set the DSCP value for IPv6 RADIUS protocol packets.

Use **undo radius ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Examples

# Set the DSCP value to 6 for IPv6 RADIUS protocol packets.

```
<Sysname> system-view
[Sysname] radius ipv6 dscp 6
```

radius nas-ip

Syntax

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

View

System view

Default level

2: System level

Parameters

ipv4-address: IPv4 address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address. It must be a unicast address of the switch that is neither a loopback address nor a link-local address.

Description

Use **radius nas-ip** to specify a source address for outgoing RADIUS packets.

Use **undo radius nas-ip** to remove the configuration.

By default, the source IP address of an outgoing RADIUS packet is the IP address of the outbound interface.

You can specify up to 16 source IP addresses.

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

The setting configured by the **nas-ip** command in RADIUS scheme view is only for the RADIUS scheme, whereas that configured by the **radius nas-ip** command in system view is for all RADIUS schemes. The setting in RADIUS scheme view takes precedence.

Related commands: **nas-ip**.

Examples

# Set the IP address for the switch to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View

System view

Default level

3: Manage level

Parameters

radius-scheme-name: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use **radius scheme** to create a RADIUS scheme and enter RADIUS scheme view.

Use **undo radius scheme** to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

A RADIUS scheme can be referenced by more than one ISP domain at the same time.

A RADIUS scheme referenced by ISP domains cannot be removed.

Related commands: **display radius scheme**.

Examples

# Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

radius trap

Syntax

radius trap { **accounting-server-down** | **authentication-error-threshold** | **authentication-server-down** }

undo radius trap { **accounting-server-down** | **authentication-error-threshold** | **authentication-server-down** }

View

System view

Default level

2: System level

Parameters

accounting-server-down: Sends traps when the reachability of the accounting server changes.

authentication-error-threshold: Sends traps when the number of authentication failures exceed the specified threshold. The threshold is represented by the ratio of the number of failed request transmission attempts to the total number of transmission attempts. It ranges from 1 to 100 and defaults to 30. This threshold can only be configured through the MIB.

authentication-server-down: Sends traps when the reachability of the authentication server changes.

Description

Use **radius trap** to enable the trap function for RADIUS.

Use **undo radius trap** to disable the trap function for RADIUS.

By default, the trap function is disabled for RADIUS.

With the trap function for RADIUS, a NAS sends a trap message in the following cases:

- The status of a RADIUS server changes. If a NAS sends a request but receives no response before the maximum number of attempts is exceeded, it places the server to blocked state and sends a trap message. If a NAS receives a response from a RADIUS server it considered unreachable, it considers that the RADIUS server is reachable again and also sends a trap message.
- The ratio of the number of failed transmission attempts to the total number of authentication request transmission attempts reaches the threshold.

Examples

# Enable the switch to send traps in response to accounting server reachability changes.

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

reset radius statistics

Syntax

reset radius statistics [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Clears the RADIUS statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset radius statistics** to clear RADIUS statistics.

Related commands: **display radius statistics**.

Examples

# Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

reset stop-accounting-buffer (for RADIUS)

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Clears buffered stop-accounting requests that are destined for the accounting server defined in a RADIUS scheme. The RADIUS scheme name is a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Clears the stop-accounting requests buffered for a session. The session ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Clears the stop-accounting requests buffered in a time range. The start time and end time must be in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD.

user-name *user-name*: Clears the stop-accounting requests buffered for a user. The username is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

slot *slot-number*: Clears the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset stop-accounting-buffer** to clear the buffered stop-accounting requests for which no responses have been received.

Related commands: **stop-accounting-buffer enable** and **display stop-accounting-buffer**.

Examples

# Clear the stop-accounting requests buffered for user **user0001@test**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@test
```

# Clear the stop-accounting requests buffered in the time range from 0:0:0 to 23:59:59 on March 31, 2011.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-03/31/2011 23:59:59-03/31/2011
```

retry

Syntax

retry *retry-times*

undo retry

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of RADIUS packet transmission attempts, in the range of 1 to 20.

Description

Use **retry** to set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.

Use **undo retry** to restore the default.

By default, the maximum number of RADIUS packet transmission attempts is 3.

Because RADIUS uses UDP packets to transmit data, the communication is not reliable. If the switch does not receive a response to its request from the RADIUS server within the response timeout period, it retransmits the RADIUS request. If the number of transmission attempts exceeds the limit but the switch still receives no response from the RADIUS server, the switch considers the request a failure.

The maximum number of packet transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme** and **timer response-timeout**.

Examples

# Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax

retry realtime-accounting *retry-times*

undo retry realtime-accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of accounting attempts, in the range of 1 to 255.

Description

Use **retry realtime-accounting** to set the maximum number of accounting attempts.

Use **undo retry realtime-accounting** to restore the default.

By default, the maximum number of accounting attempts is 5.

A RADIUS server usually checks whether a user is online by using a timeout timer. If it receives no real-time accounting request for a user in the timeout period from the NAS, it considers that there may be link or switch failures and stops accounting for the user. This may happen when some unexpected failure occurs. To cooperate with this feature of the RADIUS server, the NAS must keep pace with the server in disconnecting the user. The maximum number of accounting attempts, together with some other parameters, enables the NAS to promptly disconnect the user.

The maximum number of accounting attempts, together with some other parameters, controls how the NAS sends accounting request packets.

Suppose that the RADIUS server response timeout period is three seconds (set with the **timer response-timeout** command), the maximum number of RADIUS packet transmission attempts is three (set with the **retry** command), the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting attempts is five (set with the **retry realtime-accounting** command). In this case, the switch generates an accounting request every 12 minutes, and retransmits the request if it sends the request but receives no response within three seconds. If the switch receives no response after transmitting the request three times, it considers the accounting attempt a failure, and makes another accounting attempt. If five consecutive accounting attempts fail, the switch cuts the user connection.

Related commands: **retry**, **timer response-timeout**, and **timer realtime-accounting**.

Examples

# Set the maximum number of accounting attempts to 10 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

retry stop-accounting (RADIUS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of stop-accounting attempts, in the range of 10 to 65535.

Description

Use **retry stop-accounting** to set the maximum number of stop-accounting attempts.

Use **undo retry stop-accounting** to restore the default.

By default, the maximum number of stop-accounting attempts is 500.

The maximum number of stop-accounting attempts, together with some other parameters, controls how the NAS deals with stop-accounting request packets.

Suppose that the RADIUS server response timeout period is three seconds (set with the **timer response-timeout** command), the maximum number of transmission attempts is five (set with the **retry** command), and the maximum number of stop-accounting attempts is 20 (set with the **retry stop-accounting** command). For each stop-accounting request, if the switch receives no response within three seconds, it retransmits the request. If it receives no responses after retransmitting the request five times, it considers the stop-accounting attempt a failure, buffers the request, and makes another stop-accounting attempt. If 20 consecutive attempts fail, the switch discards the request.

Related commands: **retry**, **retry stop-accounting**, **timer response-timeout**, and **display stop-accounting-buffer**.

Examples

# Set the maximum number of stop-accounting attempts to 1000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key*] *

undo secondary accounting [*ipv4-address* | **ipv6** *ipv6-address*]

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the secondary accounting server, in dotted decimal notation.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server, which is a UDP port number in the range of 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the secondary RADIUS accounting server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **secondary accounting** to specify secondary RADIUS accounting servers for a RADIUS scheme.

Use **undo secondary accounting** to remove a secondary RADIUS accounting server.

By default, no secondary RADIUS accounting server is specified.

Make sure the port number and shared key settings of the secondary RADIUS accounting server are the same as those configured on the server.

You can configure up to 16 secondary RADIUS accounting servers for a RADIUS scheme by executing this command repeatedly. After the configuration, if the primary server fails, the switch looks for a secondary server in active state (a secondary RADIUS accounting server configured earlier has a higher priority) and tries to communicate with it.

The IP addresses of the accounting servers and those of the authentication/authorization servers must be of the same IP version.

The IP addresses of the primary and secondary accounting servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key accounting** [**cipher** | **simple**] *key* command.

If you remove a secondary accounting server when the switch has already sent a start-accounting request to the server, the communication with the secondary server times out, and the switch looks for a server in active state from the primary server on.

If you remove an accounting server being used by online users, the switch cannot send real-time accounting requests and stop-accounting requests anymore for the users, and does not buffer the stop-accounting requests.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **key**, **state**.

Examples

# For RADIUS scheme **radius1**, set the IP address of the secondary accounting server to 10.110.1.1, the UDP port to 1813, and the shared key to **$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B** in cipher text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813 key cipher
$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B
```

# For RADIUS scheme **radius2,** specify two secondary accounting servers with the server IP addresses of 10.110.1.1 and 10.110.1.2 and the UDP port number of 1813. Set the shared keys to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813 key hello
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813 key hello
```

secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] *

undo secondary authentication [*ipv4-address* | **ipv6** *ipv6-address*]

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the secondary authentication/authorization server, in dotted decimal notation.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary authentication/authorization server.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, which is a UDP port number in the range of 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the secondary RADIUS authentication/authorization server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

probe username: Enables the switch to detect the status of the secondary RADIUS authentication/authorization server.

username *name*: Specifies the username in the authentication request that is used to detect the status of the secondary RADIUS authentication/authorization server.

interval *interval*: Specifies the interval between two server status detections. The value ranges from 1 to 3600 and defaults to 60, in minutes.

Description

Use **secondary authentication** to specify secondary RADIUS authentication/authorization servers for a RADIUS scheme.

Use **undo secondary authentication** to remove a secondary RADIUS authentication/authorization server.

By default, no secondary RADIUS authentication/authorization server is specified.

Make sure the port number and shared key settings of the secondary RADIUS authentication/authorization server are the same as those configured on the server.

You can configure up to 16 secondary RADIUS authentication/authorization servers for a RADIUS scheme by executing this command repeatedly. After the configuration, if the primary server fails, the switch looks for a secondary server in active state (a secondary RADIUS authentication/authorization server configured earlier has a higher priority) and tries to communicate with it.

The IP addresses of the authentication/authorization servers and those of the accounting servers must be of the same IP version.

The IP addresses of the primary and secondary authentication/authorization servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key authentication** [**cipher** | **simple**] *key* command.

If you remove a secondary authentication server in use in the authentication process, the communication with the secondary server times out, and the switch looks for a server in active state from the primary server on.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

With the server status detection feature enabled, the switch sends an authentication request that carries the specified username to the secondary server at the specified interval. If the switch receives no response from the server within the time interval specified by the **timer response-timeout** command, the switch sends the authentication request again.

If the maximum number of retries (specified by the **retry** command) is reached and the switch still receives no response from the server, the switch considers the server as unreachable. If the switch receives a response from the server before the maximum number of retries is reached, the switch considers the server as reachable. The switch sets the status of the server to **block** or **active** according to the status detection result, regardless of the current status of the server.

For 802.1X authentication, if the status of every server is **block**, the switch assigns the port connected to an authentication user to the specified 802.1X critical VLAN. For more information about the 802.1X critical VLAN, see *Security Configuration Guide*.

To ensure that the switch can set the server to its actual status, set a longer quiet timer for the secondary server with the **timer quiet** command. If you set a short quiet timer and configure 802.1X critical VLAN on a port, the switch might frequently change the server status, and the port might frequently join and leave the critical VLAN.

Related commands: **key**, **state**.

Examples

# For RADIUS scheme **radius1**, set the IP address of the secondary authentication/authorization server to 10.110.1.2, the UDP port to 1812, and the shared key to **$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B** in cipher text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812 key cipher
$c$3$NMCbVjyIutaV6csCOGp4zsKRTlg2eT3B
```

# Specify two secondary authentication/authorization servers for RADIUS scheme **radius2**, with the server IP addresses of 10.110.1.1 and 10.110.1.2, and the UDP port number of 1813. Set the shared keys to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812 key simple hello
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812 key simple hello
```

# In RADIUS scheme **radius1**, set the username used for status detection of the secondary authentication/authorization server to **test** in plain text, and set the server status detection interval to 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.1 probe username test interval
120
```

security-policy-server

Syntax

security-policy-server *ip-address*

undo security-policy-server { *ip-address* | **all** }

View

RADIUS scheme view

Default level

2: System level

Parameters

ip-address: Specifies a security policy server by its IP address.

all: Specifies all security policy servers.

Description

Use **security-policy-server** to specify a security policy server for a RADIUS scheme.

Use **undo security-policy-server** to remove security policy servers for a RADIUS scheme.

By default, no security policy server is specified for a RADIUS scheme.

You can change security policy servers for a RADIUS scheme only when no user is using the scheme.

Examples

# Specify security policy server 10.110.1.2 for RADIUS scheme **radius1**.

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

server-type

Syntax

server-type { **extended** | **standard** }

undo server-type

View

RADIUS scheme view

Default level

2: System level

Parameters

extended: Specifies the extended RADIUS server (generally running on IMC), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the proprietary RADIUS protocol.

standard: Specifies the standard RADIUS server, which requires the RADIUS client and RADIUS server to interact according to the procedures and packet format of the standard RADIUS protocol (RFC 2865 and 2866 or their successors).

Description

Use **server-type** to configure the RADIUS server type.

Use **undo server-type** to restore the default.

By default, the supported RADIUS server type is **standard**.

Examples

# Configure the RADIUS server type of RADIUS scheme **radius1** as **standard**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type standard
```

state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the status of the primary RADIUS accounting server.

authentication: Sets the status of the primary RADIUS authentication/authorization server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Description

Use **state primary** to set the status of a primary RADIUS server.

By default, the primary RADIUS server specified for a RADIUS scheme is in active state.

During an authentication or accounting process, the switch first tries to communicate with the primary server if the primary server is in active state. If the primary server is unavailable, the switch changes the status of the primary server to blocked, starts a quiet timer for the server, and then tries to communicate with a secondary server in active state (a secondary RADIUS server configured earlier has a higher priority). When the quiet timer of the primary server times out, the status of the server changes to active automatically. If you set the status of the server to blocked before the quiet timer times out, the status of the server cannot change back to active automatically unless you set the status to active manually.

When the primary server and secondary servers are both in blocked state, the switch communicates with the primary server.

Related commands: **display radius scheme** and **state secondary**.

Examples

# Set the status of the primary server in RADIUS scheme **radius1** to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

state secondary

Syntax

state secondary { **accounting** | **authentication** } [**ip** *ipv4-address* | **ipv6** *ipv6-address*] { **active** | **block** }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the status of the secondary RADIUS accounting server.

authentication: Sets the status of the secondary RADIUS authentication/authorization server.

ip *ipv4-address*: Specifies the IPv4 address of the secondary RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Description

Use **state secondary** to set the status of a secondary RADIUS server.

By default, every secondary RADIUS server specified in a RADIUS scheme is in active state.

If no IP address is specified, this command changes the status of all configured secondary servers for authentication/authorization or accounting.

If the switch finds that a secondary server in active state is unreachable, the switch changes the status of the secondary server to blocked, starts a quiet timer for the server, and continues to try to communicate with the next secondary server in active state (a secondary RADIUS server configured earlier has a higher priority). When the quiet timer of a server times out, the status of the server changes to active automatically. If you set the status of the server to blocked before the quiet timer times out, the status of the server cannot change back to active automatically unless you set the status to active manually. If all configured secondary servers are unreachable, the switch considers the authentication or accounting attempt a failure.

Related commands: **display radius scheme** and **state primary**.

Examples

# Set the status of all the secondary servers in RADIUS scheme **radius1** to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

stop-accounting-buffer enable (RADIUS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

RADIUS scheme view

Default level

2: System level

Parameters

None

Description

Use **stop-accounting-buffer enable** to enable the switch to buffer stop-accounting requests to which no responses are received.

Use **undo stop-accounting-buffer enable** to disable the buffering function.

By default, the switch buffers stop-accounting requests to which no responses are received.

Stop-accounting requests affect the charge to users. A NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission attempts reaches the configured limit. In the latter case, the NAS discards the packet. However, if you have removed the accounting server, stop-accounting messages are not buffered.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

# Enable the switch to buffer the stop-accounting requests to which no responses are received.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

View

RADIUS scheme view

Default level

2: System level

Parameters

minutes: Server quiet period in minutes, in the range of 0 to 255. If you set this argument to 0, when the switch attempts to send an authentication or accounting request but the current server is unreachable, the switch sends the request to the next server in active state, without changing the current server's status. As a result, when the switch attempts to send a request of the same type for another user, it still tries to send the request to the current server because the current server is in active state.

Description

Use **timer quiet** to set the quiet timer for the servers. This timer controls whether the switch changes the status of an unreachable server from active to blocked, and how long the switch keeps an unreachable server in blocked state.

Use **undo timer quiet** to restore the default.

By default, the server quiet period is 5 minutes.

If you determine that the primary server is unreachable because the switch's port connected to the server is out of service temporarily or the server is busy, you can set the server quiet period to 0 so that the switch uses the primary server whenever possible.

Be sure to set the server quiet timer properly. Too short a quiet timer may result in frequent authentication or accounting failures because the switch has to repeatedly try to communicate with an unreachable server that is in active state.

Related commands: **display radius scheme**.

Examples

# Set the quiet timer for the servers to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

minutes: Real-time accounting interval in minutes, zero or a multiple of 3 in the range of 3 to 60.

Description

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

By default, the real-time accounting interval is 12 minutes.

For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command sets the interval.

When the real-time accounting interval on the switch is zero, the switch sends online user accounting information to the RADIUS accounting server at the real-time accounting interval configured on the server (if any) or does not send online user accounting information.

Different real-time accounting intervals impose different performance requirements on the NAS and the RADIUS server. A shorter interval helps achieve higher accounting precision but requires higher performance. Use a longer interval when there are a large number of users (1000 or more).

Table 7 Recommended real-time accounting intervals

Number of users	Real-time accounting interval (minutes)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or longer

Related commands: **retry realtime-accounting**.

Examples

# Set the real-time accounting interval to 51 minutes for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

RADIUS scheme view

Default level

2: System level

Parameters

seconds: RADIUS server response timeout period in seconds, in the range of 1 to 10.

Description

Use **timer response-timeout** to set the RADIUS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

By default, the RADIUS server response timeout period is 3 seconds.

If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it resends the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

The maximum number of RADIUS packet transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **retry**.

Examples

# Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

RADIUS scheme view

Default level

2: System level

Parameters

keep-original: Sends the username to the RADIUS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Description

Use **user-name-format** to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

A username is generally in the format *userid@isp-name*, of which *isp-name* is used by the switch to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the switch must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to a RADIUS server.

If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same *userid* as one.

For 802.1X users using EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect and the switch does not change the usernames from clients before forwarding them to the RADIUS server.

Related commands: **radius scheme**.

Examples

# Specify the switch to remove the domain name in the username sent to the RADIUS servers for the RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

HWTACACS configuration commands

data-flow-format (HWTACACS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

View

HWTACACS scheme view

Default level

2: System level

Parameters

data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use **data-flow-format** to set the traffic statistics unit for data flows or packets.

Use **undo data-flow-format** to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

The unit for data flows and that for packets must be consistent with those on the HWTACACS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display hwtacacs**.

Examples

# Set the traffic statistics unit for data flows and that for packets to kilobytes and kilo-packets respectively in HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

display hwtacacs

Syntax

display hwtacacs [*hwtacacs-scheme-name* [**statistics**]] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

hwtacacs-scheme-name: HWTACACS scheme name.

statistics: Displays the statistics for the HWTACACS servers specified in the HWTACACS scheme. Without this keyword, the command displays the configuration of the HWTACACS scheme.

slot *slot-number*: Specifies the configuration or statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display hwtacacs** to display the configuration of HWTACACS schemes or the statistics for the HWTACACS servers specified in HWTACACS schemes.

If no HWTACACS scheme is specified, the command displays the configuration of all HWTACACS schemes.

Related commands: **hwtacacs scheme**.

Examples

# Display the configuration of HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy
  ------------------------------------------------------------------
  HWTACACS-server template name     : gy
  Primary-authentication-server     : 172.31.1.11:49
  Primary-authorization-server      : 172.31.1.11:49
  Primary-accounting-server         : 172.31.1.11:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
```

```
Secondary-accounting-server        : 0.0.0.0:0
Current-authentication-server      : 172.31.1.11:49
Current-authorization-server       : 172.31.1.11:49
Current-accounting-server          : 172.31.1.11:49
NAS-IP-address                     : 0.0.0.0
key authentication                 : ******
key authorization                  : ******
key accounting                     : ******
Quiet-interval(min)                : 5
Realtime-accounting-interval(min)  : 12
Response-timeout-interval(sec)     : 5
Acct-stop-PKT retransmit times     : 100
Username format                    : with-domain
Data traffic-unit                  : B
Packet traffic-unit                : one-packet
--------------------------------------------------------------------
```

Table 8 Command output

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme.
Primary-authentication-server	IP address and port number of the primary authentication server. If no primary authentication server is specified, this field displays **0.0.0.0:0**. This rule also applies to the following eight fields.
Primary-authorization-server	IP address and port number of the primary authorization server.
Primary-accounting-server	IP address and port number of the primary accounting server.
Secondary-authentication-server	IP address and port number of the secondary authentication server.
Secondary-authorization-server	IP address and port number of the secondary authorization server.
Secondary-accounting-server	IP address and port number of the secondary accounting server.
Current-authentication-server	IP address and port number of the currently used authentication server.
Current-authorization-server	IP address and port number of the currently used authorization server.
Current-accounting-server	IP address and port number of the currently used accounting server.
NAS-IP-address	IP address of the NAS. If no NAS is specified, this field displays **0.0.0.0**.
key authentication	Key for authentication, displayed as a series of asterisks (******). If no shared key is configured, field displays a hyphen (**-**).
key authorization	Key for authorization, displayed as a series of asterisks (******). If no shared key is configured, field displays a hyphen (**-**).
key accounting	Key for accounting, displayed as a series of asterisks (******). If no shared key is configured, field displays a hyphen (**-**).
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission attempts.
Data traffic-unit	Unit for data flows.

Field	Description
Packet traffic-unit	Unit for data packets.

# Display the statistics for the servers specified in HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy statistics
Slot: 1
---[HWTACACS template gy primary authentication]---
HWTACACS server open number: 10
HWTACACS server close number: 10
HWTACACS authen client access request packet number: 10
HWTACACS authen client access response packet number: 6
HWTACACS authen client unknown type number: 0
HWTACACS authen client timeout number: 4
HWTACACS authen client packet dropped number: 4
HWTACACS authen client access request change password number: 0
HWTACACS authen client access request login number: 5
HWTACACS authen client access request send authentication number: 0
HWTACACS authen client access request send password number: 0
HWTACACS authen client access connect abort number: 0
HWTACACS authen client access connect packet number: 5
HWTACACS authen client access response error number: 0
HWTACACS authen client access response failure number: 0
HWTACACS authen client access response follow number: 0
HWTACACS authen client access response getdata number: 0
HWTACACS authen client access response getpassword number: 5
HWTACACS authen client access response getuser number: 0
HWTACACS authen client access response pass number: 1
HWTACACS authen client access response restart number: 0
HWTACACS authen client malformed access response number: 0
HWTACACS authen client round trip time(s): 5
---[HWTACACS template gy primary authorization]---
HWTACACS server open number: 1
HWTACACS server close number: 1
HWTACACS author client request packet number: 1
HWTACACS author client response packet number: 1
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number: 0
HWTACACS author client unknown type number: 0
HWTACACS author client request EXEC number: 1
HWTACACS author client response error number: 0
HWTACACS author client response EXEC number: 1
HWTACACS author client round trip time(s): 3
---[HWTACACS template gy primary accounting]---
HWTACACS server open number: 0
HWTACACS server close number: 0
HWTACACS account client request packet number: 0
HWTACACS account client response packet number: 0
HWTACACS account client unknown type number: 0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number: 0
HWTACACS account client request command level number: 0
HWTACACS account client request connection number: 0
HWTACACS account client request EXEC number: 0
HWTACACS account client request network number: 0
HWTACACS account client request system event number: 0
HWTACACS account client request update number: 0
HWTACACS account client response error number: 0
HWTACACS account client round trip time(s): 0
```

display stop-accounting-buffer (for HWTACACS)

Syntax

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in an HWTACACS scheme. The HWTACACS scheme name is a case-insensitive string of 1 to 32 characters.

slot *slot-number*: Specifies the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stop-accounting-buffer** to display information about buffered stop-accounting requests.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, and **retry stop-accounting**.

Examples

# Display information about stop-accounting requests buffered for HWTACACS scheme **hwt1**.

```
  Slot  1:
Total 0 record(s) Matched
```

hwtacacs nas-ip

Syntax

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip *ip-address*

View

System view

Default level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

Description

Use **hwtacacs nas-ip** to specify a source IP address for outgoing HWTACACS packets.

Use **undo hwtacacs nas-ip** to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound interface.

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, an HWTACACS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

You can specify up to 16 source IP addresses.

The setting configured by the **nas-ip** command in HWTACACS scheme view is only for the HWTACACS scheme, whereas that configured by the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. The setting in HWTACACS scheme view takes precedence.

Related commands: **nas-ip**.

Examples

# Set the IP address for the switch to use as the source address of the HWTACACS packets to **129.10.10.1**.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View

System view

Default level

3: Manage level

Parameters

hwtacacs-scheme-name: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use **hwtacacs scheme** to create an HWTACACS scheme and enter HWTACACS scheme view.

Use **undo hwtacacs scheme** to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

An HWTACACS scheme can be referenced by more than one ISP domain at the same time.

An HWTACACS scheme referenced by ISP domains cannot be removed.

Examples

# Create an HWTACACS scheme named **hwt1** and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** | **authorization** }

View

HWTACACS scheme view

Default level

2: System level

Parameters

accounting: Sets the shared key for secure HWTACACS accounting communication.

authentication: Sets the shared key for secure HWTACACS authentication communication.

authorization: Sets the shared key for secure HWTACACS authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **key** to set the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Use **undo key** to remove the configuration.

By default, no shared key is configured.

The shared keys configured on the switch must match those configured on the HWTACACS servers.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **display hwtacacs**.

Examples

# Set the shared key for secure HWTACACS accounting communication to **hello** in plain text.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting simple hello
```

# Set the shared key for secure HWTACACS accounting communication to **hello** in plain text.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

# Set the shared key for secure HWTACACS accounting communication to **$c$3$jaeN0ej15fjuHKeuVh8mqicHzaHdMw==** in cipher text.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting cipher $c$3$jaeN0ej15fjuHKeuVh8mqicHzaHdMw==
```

nas-ip (HWTACACS scheme view)

Syntax

nas-ip *ip-address*

undo nas-ip

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

Description

Use **nas-ip** to specify a source address for outgoing HWTACACS packets.

Use **undo nas-ip** to restore the default.

By default, the source IP address of an outgoing HWTACACS packet is configured by the **hwtacacs nas-ip** command in system view. If the **hwtacacs nas-ip** command is not configured, the source IP address is the IP address of the outbound interface.

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, an HWTACACS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

If you configure the command repeatedly, only the last configuration takes effect.

The setting configured by the **nas-ip** command in HWTACACS scheme view is only for the HWTACACS scheme, whereas that configured by the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. The setting in HWTACACS scheme view takes precedence.

Related commands: **hwtacacs nas-ip**.

Examples

# Set the source address for outgoing HWTACACS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

primary accounting (HWTACACS scheme view)

Syntax

primary accounting *ip-address* [*port-number*] *

undo primary accounting

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS accounting server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS accounting server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary accounting** to specify the primary HWTACACS accounting server.

Use **undo primary accounting** to remove the configuration.

By default, no primary HWTACACS accounting server is specified.

The IP addresses of the primary and secondary accounting servers must be different. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an accounting server only when it is not used by any active TCP connection to send accounting packets. Removing an accounting server affects only accounting processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

# Specify the IP address and port number of the primary accounting server for HWTACACS scheme **test1** as 10.163.155.12 and 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication (HWTACACS scheme view)

Syntax

primary authentication *ip-address* [*port-number*] *

undo primary authentication

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS authentication server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS authentication server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary authentication** to specify the primary HWTACACS authentication server.

Use **undo primary authentication** to remove the configuration.

By default, no primary HWTACACS authentication server is specified.

The IP addresses of the primary and secondary authentication servers must be different. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an authentication server only when it is not used by any active TCP connection to send authentication packets. Removing an authentication server affects only authentication processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

# Specify the IP address and port number of the primary authentication server for HWTACACS scheme **hwt1** as 10.163.155.13 and 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax

primary authorization *ip-address* [*port-number*] *

undo primary authorization

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS authorization server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS authorization server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary authorization** to specify the primary HWTACACS authorization server.

Use **undo primary authorization** to remove the configuration.

By default, no primary HWTACACS authorization server is specified.

The IP addresses of the primary and secondary authorization servers must be different. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an authorization server only when it is not used by any active TCP connection to send authorization packets. Removing an authorization server affects only authorization processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

# Configure the IP address and port number of the primary authorization server for HWTACACS scheme **hwt1** as 10.163.155.13 and 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** } [**slot** *slot-number*]

View

User view

Default level

1: Monitor level

Parameters

accounting: Clears HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears HWTACACS authentication statistics.

authorization: Clears HWTACACS authorization statistics.

slot *slot-number*: Clears HWTACACS statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset hwtacacs statistics** to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

Examples

# Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer (for HWTACACS)

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in an HWTACACS scheme. The HWTACACS scheme name is a case-insensitive string of 1 to 32 characters.

slot *slot-number*: Clears the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset stop-accounting-buffer** to clear buffered stop-accounting requests that get no responses.

Related commands: **stop-accounting-buffer enable** and **display stop-accounting-buffer**.

Examples

# Clear the stop-accounting requests buffered for HWTACACS scheme **hwt1**.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting (HWTACACS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

HWTACACS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of stop-accounting request transmission attempts, in the range of 1 to 300.

Description

Use **retry stop-accounting** to set the maximum number of stop-accounting request transmission attempts.

Use **undo retry stop-accounting** to restore the default.

By default, the maximum number of stop-accounting request transmission attempts is 100.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

# Set the maximum number of stop-accounting request transmission attempts to 50 for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting (HWTACACS scheme view)

Syntax

secondary accounting *ip-address* [*port-number*] *

undo secondary accounting

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS accounting server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS accounting server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary accounting** to specify the secondary HWTACACS accounting server.

Use **undo secondary accounting** to remove the configuration.

By default, no secondary HWTACACS accounting server is specified.

The IP addresses of the primary and secondary accounting servers must be different. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an accounting server only when it is not used by any active TCP connection to send accounting packets. Removing an accounting server affects only accounting processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

# Specify the IP address and port number of the secondary accounting server for HWTACACS scheme **hwt1** as 10.163.155.12 with TCP port number 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication (HWTACACS scheme view)

Syntax

secondary authentication *ip-address* [*port-number*] *

undo secondary authentication

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS authentication server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS authentication server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary authentication** to specify the secondary HWTACACS authentication server.

Use **undo secondary authentication** to remove the configuration.

By default, no secondary HWTACACS authentication server is specified.

The IP addresses of the primary and secondary authentication servers must be different. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an authentication server only when it is not used by any active TCP connection to send authentication packets is using it. Removing an authentication server affects only authentication processes that occur after the remove operation.

Related commands: **display hwtacacs** .

Examples

# Specify the IP address and port number of the secondary authentication server for HWTACACS scheme **hwt1** as 10.163.155.13 with TCP port number 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax

secondary authorization *ip-address* [*port-number*] *

undo secondary authorization

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS authorization server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS authorization server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary authorization** to specify the secondary HWTACACS authorization server.

Use **undo secondary authorization** to remove the configuration.

By default, no secondary HWTACACS authorization server is specified.

The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.

If you configure the command repeatedly, only the last configuration takes effect.

You can remove an authorization server only when it is not used by any active TCP connection to send authorization packets. Removing an authorization server affects only authorization processes that occur after the remove operation.

Related commands: **display hwtacacs** .

Examples

# Configure the secondary authorization server 10.163.155.13 with TCP port number 49.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable (HWTACACS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

HWTACACS scheme view

Default level

2: System level

Parameters

None

Description

Use **stop-accounting-buffer enable** to enable the switch to buffer stop-accounting requests to which no responses are received.

Use **undo stop-accounting-buffer enable** to disable the buffering function.

By default, the switch buffers stop-accounting requests to which no responses are received.

Stop-accounting requests affect the charge to users. A NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission attempts reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

# In HWTACACS scheme **hwt1**, enable the switch to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

timer quiet (HWTACACS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

View

HWTACACS scheme view

Default level

2: System level

Parameters

minutes: Primary server quiet period. The value ranges from 1 to 255, in minutes.

Description

Use **timer quiet** to set the quiet timer for the primary server. When the primary server is found unreachable, the switch changes the status of the server from active to blocked and keeps the server in blocked state until this timer expires.

Use **undo timer quiet** to restore the default.

By default, the primary server quiet period is 5 minutes.

Related commands: **display hwtacacs**.

Examples

# Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

timer realtime-accounting (HWTACACS scheme view)

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

HWTACACS scheme view

Default level

2: System level

Parameters

minutes: Real-time accounting interval in minutes, zero or a multiple of 3 in the range of 3 to 60. A value of zero means "Do not send online user accounting information to the HWTACACS server."

Description

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

By default, the real-time accounting interval is 12 minutes.

For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.

Consider the performance of the NAS and the HWTACACS server when you set the real-time accounting interval. A shorter interval requires higher performance. Use a longer interval when there are a large number of users (more than 1000, inclusive).

Table 9 Recommended real-time accounting intervals

Number of users	Real-time accounting interval (minutes)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Examples

# Set the real-time accounting interval to 51 minutes for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout (HWTACACS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

HWTACACS scheme view

Default level

2: System level

Parameters

seconds: HWTACACS server response timeout period in seconds, in the range of 1 to 300.

Description

Use **timer response-timeout** to set the HWTACACS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

By default, the HWTACACS server response timeout time is 5 seconds.

HWTACACS is based on TCP. When the server response timeout timer or the TCP timeout timer times out, the switch is disconnected from the HWTACACS server.

Related commands: **display hwtacacs**.

Examples

# Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format (HWTACACS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

HWTACACS scheme view

Default level

2: System level

Parameters

keep-original: Sends the username to the HWTACACS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Description

Use **user-name-format** to specify the format of the username to be sent to an HWTACACS server.

By default, the ISP domain name is included in the username.

A username is generally in the format *userid@isp-name*, of which *isp-name* is used by the switch to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such an HWTACACS server, the switch must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to an HWTACACS server.

If an HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same *userid* as one.

Examples

# Specify the switch to remove the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

RADIUS server configuration commands

authorization-attribute (RADIUS-server user view)

Syntax

authorization-attribute { **acl** *acl-number* | **vlan** *vlan-id* } *

undo authorization-attribute { **acl** | **vlan** } *

View

RADIUS-server user view

Default level

2: System level

Parameters

acl *acl-number*: Specifies the number of an ACL in the range of 2000 to 5999.

vlan *vlan-id*: Specifies the ID of a VLAN in the range of 1 to 4094.

Description

Use **authorization-attribute** to specify the authorization attributes (ACL and VLAN) that the RADIUS server assigns to the RADIUS client in a response message after the RADIUS user passes RADIUS authentication. The RADIUS client uses the assigned authorization attributes to control the access of the RADIUS user.

Use **undo authorization-attribute** to remove the configuration.

By default, no authorization attribute is configured.

Related commands: **radius-server user**.

Examples

# Configure the authorized VLAN for RADIUS user **user1** as VLAN 3.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] authorization-attribute vlan 3
```

description (RADIUS-server user view)

Syntax

description *text*

undo description

View

RADIUS-server user view

Default level

2: System level

Parameters

text: Description of the RADIUS user, a case-sensitive string of 1 to 255 characters.

Description

Use **description** to configure a description for the RADIUS user. The description is used for user information management.

Use **undo description** to remove the user description.

By default, no description is configured for the RADIUS user.

Related commands: **radius-server user**.

Examples

# Configure a description of **VIP user** for RADIUS user **user1**.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] description VIP user
```

expiration-date (RADIUS-server user view)

Syntax

expiration-date *time*

undo expiration-date

View

RADIUS-server user view

Default level

2: System level

Parameters

time: Expiration time of the RADIUS user, in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **expiration-date** to configure the expiration time of a RADIUS user.

Use **undo expiration-date** to remove the configuration.

By default, a RADIUS user has no expiration time and no expiration check is performed.

For temporary network access requirements, create a guest account for the user and specify an expiration time for the account. After the user passes authentication, the RADIUS server checks whether the current system time is before the expiration time. If yes, it permits the user to access the network. Otherwise, it denies the access request of the user.

If you change the system time manually or the system time is changed in any other way, the switch uses the new system time for expiration check.

Related commands: **radius-server user**.

Examples

# Configure user **user1** to expire in 12:10:20 on May 31, 2012.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] expiration-date 12:10:20-2012/05/31
```

password (RADIUS-server user view)

Syntax

password [**cipher** | **simple**] *password*

undo password

View

RADIUS-server user view

Default level

2: System level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 128 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 201 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Description

Use **password** to configure a password for the RADIUS user.

Use **undo password** to delete the password of the RADIUS user.

By default, no password is configured for the RADIUS user.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Related commands: **radius-server user**.

Examples

# Set the password of **user1** to 123456 in plain text.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] password simple 123456
```

# Set the password of **user2** to **$c$3$joGi2vMNJMbTEjpMA1J7Nuv2+iif3Q==** in cipher text.

```
<Sysname> system-view
[Sysname] radius-server user user2
[Sysname-rdsuser-user2] password cipher $c$3$joGi2vMNJMbTEjpMA1J7Nuv2+iif3Q==
```

radius-server client-ip

Syntax

radius-server client-ip *ip-address* [**key** [**cipher** | **simple**] *string*]

undo radius-server client-ip { *ip-address* | **all** }

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IPv4 address of the RADIUS client.

key: Sets the shared key for secure communication with the RADIUS client.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

all: Specifies all RADIUS clients.

Description

Use **radius-server client-ip** to specify a RADIUS client.

Use **undo radius-server client-ip** to delete the specified RADIUS client or all RADIUS clients.

The IP address of the RADIUS client specified on the RADIUS server must be consistent with the source IP address of RADIUS packets configured on the RADIUS client.

The shared key specified on the RADIUS serer must be consistent with that configured on the RADIUS client.

To specify multiple RADIUS clients, execute this command repeatedly.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Examples

# Specify RADIUS client 10.1.1.1 and set the shared key to 1234 in plain text.

```
<Sysname> system-view
[Sysname] radius-server client-ip 10.1.1.1 key simple 1234
```

radius-server user

Syntax

radius-server user *user-name*

undo radius-server user { *user-name* | **all** }

View

System view

Default level

2: System level

Parameters

user-name: *user-name*: RADIUS username, a case-sensitive string of 1 to 64 characters that can contain the domain name. It cannot contain question mark (?), left angle bracket (<), right angle bracket (>), backslash (\), quotation marks ("), percent sign (%), apostrophe ('), ampersand (&), pound sign (#), or spaces, and cannot be **a**, **al**, or **all**.

all: Removes all RADIUS users.

Description

Use **radius-server user** to create a RADIUS user and enter RADIUS-server user view.

Use **undo radius-server user** to delete the specified RADIUS user or all RADIUS users.

By default, no RADIUS user exists.

If the switch is configured to send usernames that carry the domain name to the RADIUS server, the username of the RADIUS user configured here must contain the domain name. If not, the username of the RADIUS user configured here does not contain the domain name.

Related commands: **user-name-format** (RADIUS scheme view).

Examples

# Create RADIUS user **user1** and enter its view.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1]
```

802.1X configuration commands

display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two interfaces must be the same type.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dot1x** to display information about 802.1X.

If you specify neither the **sessions** keyword nor the **statistics** keyword, the command displays all information about 802.1X, including session information, statistics, and configurations.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, and **dot1x timer**.

Examples

# Display all information about 802.1X.

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
EAD quick deploy is enabled
```

```
Configuration: Transmit Period     30 s,  Handshake Period       15 s
               Quiet Period        60 s,  Quiet Period Timer is disabled
               Supp Timeout        30 s,  Server Timeout         100 s
               Reauth Period     3600 s
               The maximal retransmitting times          3
EAD quick deploy configuration:
               URL: http://192.168.19.23
               Free IP: 192.168.19.0 255.255.255.0
               EAD timeout:    30m

The maximum 802.1X user resource number is 1024 per slot
Total current used 802.1X resource number is 1

GigabitEthernet1/0/1  is link-up
  802.1X protocol is enabled
  Handshake is disabled
  Handshake secure is disabled
  802.1X unicast-trigger is enabled
  Periodic reauthentication is disabled
  The port is an authenticator
  Authenticate Mode is Auto
  Port Control Type is Mac-based
  802.1X Multicast-trigger is enabled
  Mandatory authentication domain: NOT configured
  Guest VLAN: 4
  Auth-fail VLAN: NOT configured
  Critical VLAN: 3
  Critical recovery-action: reinitialize
  Max number of on-line users is 256

  EAPOL Packet: Tx 1087, Rx 986
  Sent EAP Request/Identity Packets : 943
       EAP Request/Challenge Packets: 60
       EAP Success Packets: 29, Fail Packets: 55
  Received EAPOL Start Packets : 60
           EAPOL LogOff Packets: 24
           EAP Response/Identity Packets : 724
           EAP Response/Challenge Packets: 54
           Error Packets: 0
1. Authenticated user : MAC address: 0015-e9a6-7cfe

  Controlled User(s) amount to 1
```

Table 10 Command output

Field	Description
Equipment 802.1X protocol is enabled	Specifies whether 802.1X is enabled globally
CHAP authentication is enabled	Specifies whether CHAP authentication is enabled
EAD quick deploy is enabled	Specifies whether EAD fast deployment is enabled
Transmit Period	Username request timeout timer in seconds
Handshake Period	Handshake timer in seconds
Reauth Period	Periodic online user re-authentication timer in seconds
Quiet Period	Quiet timer in seconds
Quiet Period Timer is disabled	Status of the quiet timer. In this example, the quiet timer is enabled.
Supp Timeout	Client timeout timer in seconds
Server Timeout	Server timeout timer in seconds
The maximal retransmitting times	Maximum number of attempts for sending an authentication request to a client
EAD quick deploy configuration	EAD fast deployment configuration
URL	Redirect URL for unauthenticated users using a web browser to access the network
Free IP	Freely accessible network segment
EAD timeout	EAD rule timer in minutes
The maximum 802.1X user resource number per slot	Maximum number of concurrent 802.1X user per card
Total current used 802.1X resource number	Total number of online 802.1X users
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X protocol is disabled	Specifies whether 802.1X is enabled on the port
Handshake is disabled	Specifies whether handshake is enabled on the port
Handshake secure is disabled	Specifies whether handshake security is enabled on the port
802.1X unicast-trigger is disabled	Specifies whether unicast trigger is enabled on the port.
Periodic reauthentication is disabled	Specifies whether periodic online user re-authentication is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Authorization state of the port
Port Control Type is Mac-based	Access control method of the port
802.1X Multicast-trigger is enabled	Specifies whether the 802.1X multicast-trigger function is enabled
Mandatory authentication domain	Mandatory authentication domain on the port
Guest VLAN	802.1X guest VLAN configured on the port. **NOT configured** is displayed if no guest VLAN is configured.

Field	Description
Auth-fail VLAN	Auth-Fail VLAN configured on the port. **NOT configured** is displayed if no Auth-Fail VLAN is configured.
Critical VLAN	802.1X critical VLAN configured on the port. **NOT configured** is displayed if no 802.1X critical VLAN is configured on the port.
Critical recovery-action	Action that the port takes when an active (reachable) authentication server is detected available for the 802.1X users in the critical VLAN: **reinitialize**—The port triggers authentication. **NOT configured**—The port does not trigger authentication.
Max number of on-line users	Maximum number of concurrent 802.1X users on the port
EAPOL Packet	Number of sent (Tx) and received (Rx) EAPOL packets
Sent EAP Request/Identity Packets	Number of sent EAP-Request/Identity packets
EAP Request/Challenge Packets	Number of sent EAP-Request/Challenge packets
EAP Success Packets	Number of sent EAP Success packets
Fail Packets	Number of sent EAP-Failure packets
Received EAPOL Start Packets	Number of received EAPOL-Start packets
EAPOL LogOff Packets	Number of received EAPOL-LogOff packets
EAP Response/Identity Packets	Number of received EAP-Response/Identity packets
EAP Response/Challenge Packets	Number of received EAP-Response/Challenge packets
Error Packets	Number of received error packets
Authenticated user	User that has passed 802.1X authentication
Controlled User(s) amount	Number of authenticated users on the port

dot1x

Syntax

In system view:

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

In Ethernet interface view:

dot1x

undo dot1x

View

System view, Ethernet interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x** in system view to enable 802.1X globally.

Use **undo dot1x** in system view to disable 802.1X globally.

Use **dot1x interface** in system view or **dot1x** in interface view to enable 802.1X for specified ports.

Use **undo dot1x interface** in system view or the **undo dot1x** command in interface view to disable 802.1X for specified ports.

By default, 802.1X is neither enabled globally nor enabled for any port.

802.1X must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.

You can configure 802.1X parameters either before or after enabling 802.1X.

Related commands: **display dot1x**.

Examples

# Enable 802.1X for ports GigabitEthernet 1/0/1, and GigabitEthernet 1/0/5 to GigabitEthernet 1/0/7.

```
<Sysname> system-view
[Sysname] dot1x interface gigabitethernet 1/0/1 gigabitethernet 1/0/5 to gigabitethernet
1/0/7
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/5
[Sysname-GigabitEthernet1/0/5] dot1x
[Sysname-GigabitEthernet1/0/5] quit
[Sysname] interface gigabitethernet 1/0/6
[Sysname-GigabitEthernet1/0/6] dot1x
[Sysname-GigabitEthernet1/0/6] quit
[Sysname] interface gigabitethernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x
```

# Enable 802.1X globally.

```
<Sysname> system-view
[Sysname] dot1x
```

dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

View

System view

Default level

2: System level

Parameters

chap: Sets the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Sets the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Sets the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Description

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

By default, the network access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

The network access device terminates or relays EAP packets:

1. In EAP termination mode, the access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server, and performs either CHAP or PAP authentication with the RADIUS server. In this mode the RADIUS server supports only MD5-Challenge EAP authentication, and "username+password" EAP authentication initiated by an iNode client.

- PAP transports usernames and passwords in clear text. The authentication method applies to scenarios that do not require high security. To use PAP, the client must be an HP iNode 802.1X client.
- CHAP transports username in plaintext and encrypted password over the network. It is more secure than PAP.

2. In EAP relay mode, the access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TL, and PEAP. To use this mode, you must make sure that the RADIUS server supports the EAP-Message and Message-Authenticator attributes, and uses the same EAP authentication method as the client. If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "RADIUS configuration commands."

Local authentication supports PAP and CHAP.

If RADIUS authentication is used, you must configure the network access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Related commands: **display dot1x**.

Examples

# Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Sysname> system-view
```

```
[Sysname] dot1x authentication-method pap
```

dot1x auth-fail vlan

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

View

Ethernet interface view

Default level

2: System level

Parameters

authfail-vlan-id: Specifies the ID of the Auth-Fail VLAN for the port, in the range of 1 to 4094. Make sure that the VLAN has been created.

Descriptions

Use **dot1x auth-fail vlan** to configure an Auth-Fail VLAN for a port. An Auth-Fail VLAN accommodates users that have failed 802.1X authentication because of the failure to comply with the organization security strategy, such as using a wrong password.

Use **undo dot1x auth-fail vlan** to restore the default.

By default, no Auth-Fail VLAN is configured on a port.

You must enable MAC-based VLAN for an Auth-Fail VLAN to take effect on a port that performs MAC-based access control.

When you change the access control method from MAC-based to port-based on a port that carries an Auth-Fail VLAN, the mappings between MAC addresses and the 802.1X Auth-Fail VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

You must enable 802.1X multicast trigger function for an Auth-Fail VLAN to take effect on a port that performs port-based access control.

When you change the access control method from port-based to MAC-based on a port that is in an Auth-Fail VLAN, the port is removed from the Auth-Fail VLAN.

To delete a VLAN that has been configured as an Auth-Fail VLAN, you must remove the Auth-Fail VLAN configuration first.

Related commands: **dot1x** and **dot1x port-method**.

Examples

# Configure VLAN 3 as the Auth-Fail VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 3
```

dot1x critical vlan

Syntax

dot1x critical vlan *vlan-id*

undo dot1x critical vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Description

Use **dot1x critical vlan** to configure an 802.1X critical VLAN on a port for 802.1X users that have failed authentication because all the RADIUS authentication servers in their ISP domain are unreachable.

Use **undo dot1x critical vlan** to restore the default.

By default, no 802.1X critical VLAN is configured on a port.

The 802.1X critical VLAN configuration applies to 802.1X users that use only RADIUS authentication servers and have failed authentication because all the servers in their ISP domain become unavailable (inactive), for example, for the loss of network connectivity. If an 802.1X user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

You can configure only one 802.1X critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.

Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X critical VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.

To have the 802.1X critical VLAN take effect, complete the following tasks:

- Enable 802.1X both globally and on the interface.
- If the port performs port-based access control, enable the 802.1X multicast trigger function.
- If the port performs MAC-based access control, configure the MAC-based VLAN function on the port.

When you change the access control method from MAC-based to port-based on the port, the mappings between MAC addresses and the 802.1X critical VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

When you change the access control method from port-based to MAC-based on a port that is in a critical VLAN, the port is removed from the critical VLAN.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must remove the 802.1X critical VLAN configuration first.

Related commands: **dot1x**, **dot1x port-method**, and **dot1x critical recovery-action**.

Examples

# Specify VLAN 3 as the 802.1X critical VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 3
```

dot1x critical recovery-action

Syntax

dot1x critical recovery-action reinitialize

undo dot1x critical recovery-action

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

reinitialize: Enables the port to trigger 802.1X re-authentication on detection of a reachable RADIUS authentication server for users in the critical VLAN.

Description

Use **dot1x critical recovery-action** to configure the action that a port takes when an active (reachable) RADIUS authentication server is detected for users in the critical VLAN.

Use **undo dot1x critical recovery-action** to restore the default.

By default, when a reachable RADIUS server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.

The **dot1x critical recovery-action** command takes effect only for the 802.1X users in the critical VLAN on a port. It enables the port to take one of the following actions to trigger 802.1X authentication after removing 802.1X users from the critical VLAN on detection of a reachable RADIUS authentication server:

- If MAC-based access control is used, the port sends a unicast Identity EAP/Request to each 802.1X user.
- If port-based access control is used, the port sends a multicast Identity EAP/Request to all the 802.1X users attached to the port.

For prompt detection of active RADIUS authentication servers, use RADIUS server probing function (see "AAA configuration").

Examples

# Configure port GigabitEthernet 1/0/1 to trigger 802.1X re-authentication on detection of an active RADIUS authentication server for users in the critical VLAN.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical recovery-action reinitialize
```

dot1x domain-delimiter

Syntax

dot1x domain-delimiter *string*

undo dot1x domain-delimiter

View

System view

Default level

2: System level

Parameters

string: Specifies a set of 1 to 16 domain name delimiters for 802.1X users. No space is required between delimiters. Available delimiters include the at sign (@), backslash (/), and forward slash (\).

Description

Use **dot1x domain-delimiter** to specify a set of domain name delimiters supported by the access device. Any character in the configured set can be used as the domain name delimiter for 802.1X authentication users.

Use **undo dot1x domain-delimiter** to restore the default.

By default, the access device supports only the at sign (@) delimiter for 802.1X users.

The delimiter set you configured overrides the default setting. If @ is not included in the delimiter set, the access device will not support the 802.1X users that use @ as the domain name delimiter.

If a username string contains multiple configured delimiters, the leftmost delimiter is the domain name delimiter. For example, if you configure @, /, and \ as delimiters, the domain name delimiter for the username string 123/22\@abc is the forward slash (/).

The **cut connection user-name** *user-name* and **display connection user-name** *user-name* commands are not available for 802.1X users that use / or \ as the domain name delimiter. For more information about the two commands, see "AAA configuration commands."

Examples

# Specify the characters @, /, and \ as domain name delimiters.

```
<Sysname> system-view
[Sysname] dot1x domain-delimiter @\/
```

dot1x guest-vlan

Syntax

In system view:

dot1x guest-vlan *guest-vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In Ethernet interface view:

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

View

System view, Ethernet interface view

Default level

2: System level

Parameters

guest-vlan-id: Specifies the ID of the VLAN to be specified as the 802.1X guest VLAN, in the range of 1 to 4094. Make sure that the VLAN has been created.

interface *interface-list*: Specifies a port list. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type. If no interface is specified, you configure an 802.1X guest VLAN for all Layer 2 Ethernet ports.

Description

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN for the specified or all ports.

Use **undo dot1x guest-vlan** to remove the 802.1X guest VLAN on the specified or all ports.

By default, no 802.1X guest VLAN is configured on a port.

You must enable 802.1X for an 802.1X guest VLAN to take effect.

To have the 802.1X guest VLAN take effect, complete the following tasks:

- Enable 802.1X both globally and on the interface.
- If the port performs port-based access control, enable the 802.1X multicast trigger function.
- If the port performs MAC-based access control, configure the MAC-based VLAN function on the port.

When you change the access control method from MAC-based to port-based on a port that carries a guest VLAN, the mappings between MAC addresses and the 802.1X guest VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

When you change the access control method from port-based to MAC-based on a port that is in a guest VLAN, the port is removed from the guest VLAN.

To delete a VLAN that has been configured as a guest VLAN, you must remove the guest VLAN configuration first.

Related commands: **dot1x**, **dot1x port-method**, and **dot1x multicast-trigger**; **mac-vlan enable** and **display mac-vlan** (*Layer 2—LAN Switching Command Reference*).

Examples

# Specify VLAN 999 as the 802.1X guest VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface gigabitethernet 1/0/1
```

# Specify VLAN 10 as the 802.1X guest VLAN for ports GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

# Specify VLAN 7 as the 802.1X guest VLAN for all ports.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

# Specify VLAN 3 as the 802.1X guest VLAN for port GigabitEthernet 1/0/7.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

View

Ethernet Interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x handshake** to enable the online user handshake function. The function enables the device to periodically send handshake messages to the client to check whether a user is online.

Use **undo dot1x handshake** to disable the function.

By default, the function is enabled.

HP recommends that you use the iNode client software to guarantee the normal operation of the online user handshake function.

Examples

# Enable the online user handshake function.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake
```

dot1x handshake secure

Syntax

dot1x handshake secure

undo dot1x handshake secure

View

Ethernet Interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x handshake secure** to enable the online user handshake security function. The function enables the device to prevent users from using illegal client software.

Use **undo dot1x handshake secure** to disable the function.

By default, the function is disabled.

The online user handshake security function is implemented based on the online user handshake function. To bring the security function into effect, make sure the online user handshake function is enabled.

HP recommends you use the iNode client software and IMC server to guarantee the normal operation of the online user handshake security function.

Related commands: **dot1x handshake**.

Examples

# Enable the online user handshake security function.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake secure
```

dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

View

Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters. The specified domain must already exist.

Description

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to remove the mandatory authentication domain.

By default, no mandatory authentication domain is specified.

When authenticating an 802.1X user trying to access the port, the system selects an authentication domain in the following order: the mandatory domain, the ISP domain specified in the username, and the default ISP domain.

To display or cut all 802.1X connections in a mandatory domain, use the **display connection domain** *isp-name* or **cut connection domain** *isp-name* command. The output from the **display connection** command without any parameters displays domain names input by users at login. For more information about the **display connection** command or the **cut connection** command, see "AAA configuration commands."

Related commands: **display dot1x**.

Examples

# Configure the mandatory authentication domain **my-domain** for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

# After 802.1X user **usera** passes the authentication, execute the **display connection** command to display the user connection information on GigabitEthernet 1/0/1. For more information about the **display connection** command, see "AAA configuration commands."

```
[Sysname-GigabitEthernet1/0/1] display connection interface gigabitethernet 1/0/1
Slot:  1
Index=68  ,Username=usera@my-domian
 IP=3.3.3.3
 IPv6=N/A
 MAC=0015-e9a6-7cfe

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

dot1x max-user

Syntax

In system view:

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

In Ethernet interface view:

dot1x max-user *user-number*

undo dot1x max-user

View

System view, Ethernet interface view

Default level

2: System level

Parameters

user-number: Specifies the maximum number of concurrent 802.1X users on a port. The value is in the range of 1 to 256.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

By default, the maximum number of concurrent 802.1X users on a port is 256.

In system view:

- If you do not specify the *interface-list* argument, the command applies to all ports.

- If you specify the *interface-list* argument, the command applies to the specified ports.

In Ethernet interface view, the *interface-list* argument is not available and the command applies to only the Ethernet port.

Related commands: **display dot1x**.

Examples

# Set the maximum number of concurrent 802.1X users on port GigabitEthernet 1/0/1 to 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

# Configure GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 each to support a maximum of 32 concurrent 802.1X users.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger function. The device acts as the initiator and periodically multicasts Identify EAP-Request packets out of a port to detect 802.1X clients and trigger authentication.

Use **undo dot1x multicast-trigger** to disable the function.

By default, the multicast trigger function is enabled.

You can use the **dot1x timer tx-period** command to set the interval for sending multicast Identify EAP-Request packets.

Related commands: **display dot1x**.

Examples

# Enable the multicast trigger function on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x multicast-trigger
```

dot1x port-control

Syntax

In system view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

View

System view, Ethernet interface view

Default level

2: System level

Parameters

authorized-force: Places the specified or all ports in the authorized state, enabling users on the ports to access the network without authentication.

auto: Places the specified or all ports initially in the unauthorized state to allow only EAPOL packets to pass, and after a user passes authentication, sets the port in the authorized state to allow access to the network. You can use this option in most scenarios.

unauthorized-force: Places the specified or all ports in the unauthorized state, denying any access requests from users on the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x port-control** to set the authorization state for the specified or all ports.

Use **undo dot1x port-control** to restore the default.

The default port authorization state is **auto**.

In system view, if no *interface-list* argument is specified, the command applies to all ports.

Related commands: **display dot1x**.

Examples

# Set the authorization state of port GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

# Set the authorization state of ports GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 1/0/2 to
gigabitethernet 1/0/5
```

dot1x port-method

Syntax

In system view:

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

View

System view, Ethernet interface view

Default level

2: System level

Parameters

macbased: Uses MAC-based access control on a port to separately authenticate each user attempting to access the network. In this approach, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on a port. In this approach, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges for this argument. The start port number must be smaller than the end number and the two ports must be the same type.

Description

Use **dot1x port-method** to specify an access control method for the specified or all ports.

Use **undo dot1x port-method** to restore the default.

By default, MAC-based access control applies.

In system view, if no *interface-list* argument is specified, the command applies to all ports.

Related commands: **display dot1x**.

Examples

# Configure port GigabitEthernet 1/0/1 to implement port-based access control.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

# Configure ports GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 to implement port-based access control.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface gigabitethernet 1/0/2 to gigabitethernet
1/0/5
```

dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

View

System view

Default level

2: System level

Parameters

None

Description

Use **dot1x quiet-period** to enable the quiet timer. When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client.

Use **undo dot1x quiet-period** to disable the timer.

By default, the quiet timer is disabled.

Related commands: **display dot1x** and **dot1x timer**.

Examples

# Enable the quiet timer.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x re-authenticate** to enable the periodic online user re-authentication function.

Use **undo dot1x re-authenticate** to disable the function.

By default, the periodic online user re-authentication function is disabled.

Periodic re-authentication enables the access device to periodically authenticate online 802.1X users on a port. This function tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL, VLAN, and user profile-based QoS.

You can use the **dot1x timer reauth-period** command to configure the interval for re-authentication.

Related commands: **dot1x timer reauth-period**.

Examples

# Enable the 802.1X periodic online user re-authentication function on GigabitEthernet 1/0/1 and set the periodic re-authentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

dot1x retry

Syntax

dot1x retry *max-retry-value*

undo dot1x retry

View

System view

Default level

2: System level

Parameters

max-retry-value: Specifies the maximum number of attempts for sending an authentication request to a client, in the range of 1 to 10.

Description

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

By default, the maximum number of attempts that the device can send an authentication request to a client is twice.

After the network access device sends an authentication request to a client, if the device receives no response from the client within the username request timeout timer (set with the **dot1x timer tx-period** *tx-period-value* command) or the client timeout timer (set with the **dot1x timer supp-timeout** *supp-timeout-value* command), the device retransmits the authentication request. The network access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

This command applies to all ports of the device.

Related commands: **display dot1x**.

Examples

# Set the maximum number of attempts for sending an authentication request to a client as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

View

System view

Default level

2: System level

Parameters

handshake-period-value: Sets the handshake timer in seconds, in the range of 5 to 1024.

quiet-period-value: Sets the quiet timer in seconds, in the range of 10 to 120.

reauth-period-value: Sets the periodic re-authentication timer in seconds, in the range of 60 to 7200.

server-timeout-value: Sets the server timeout timer in seconds, in the range of 100 to 300.

supp-timeout-value: Sets the client timeout timer in seconds, in the range of 1 to 120.

tx-period-value: Sets the username request timeout timer in seconds, in the range of 10 to 120.

Description

Use **dot1x timer** to set 802.1X timers.

Use **undo dot1x timer** to restore the defaults.

By default, the handshake timer is 15 seconds, the quiet timer is 60 seconds, the periodic re-authentication timer is 3600 seconds, the server timeout timer is 100 seconds, the client timeout timer is 30 seconds, and the username request timeout timer is 30 seconds.

You can set the client timeout timer to a high value in a low-performance network, set the quiet timer to a high value in a vulnerable network or a low value for quicker authentication response, or adjust the server timeout timer to adapt to the performance of different authentication servers. In most cases, the default settings are sufficient.

The network device uses the following 802.1X timers:

- Handshake timer (**handshake-period**)—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device receives no response after sending the maximum number of handshake requests, it considers that the client has logged off.
- Quiet timer (**quiet-period**)—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- Periodic re-authentication timer (**reauth-period**)—Sets the interval at which the network device periodically re-authenticates online 802.1X users. To enable periodic online user re-authentication on a port, use the **dot1x re-authenticate** command. The change to the periodic re-authentication timer applies to the users that have been online only after the old timer expires.
- Server timeout timer (**server-timeout**)—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.
- Client timeout timer **(supp-timeout**)—Starts when the access device sends an EAP-Request/MD5 Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- Username request timeout timer (**tx-period**)—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device receives no response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

Related commands: **display dot1x**.

Examples

# Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

dot1x unicast-trigger

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x unicast-trigger** to enable the 802.1X unicast trigger function.

Use **undo dot1x unicast-trigger** to disable the function.

By default, the unicast trigger function is disabled.

The unicast trigger function enables the network access device to initiate 802.1X authentication when it receives a data frame from an unknown source MAC address. The device sends a unicast Identity EAP/Request packet to the unknown source MAC address, and retransmits the packet if it has received no response within a period of time (set with the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set with the **dot1x retry** command) is reached.

Related commands: **display dot1x**, **dot1x timer tx-period**, and **dot1x retry**.

Examples

# Enable the unicast trigger function for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x unicast-trigger
```

reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-list*]

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **reset dot1x statistics** to clear 802.1X statistics.

If a list of ports is specified, the command clears 802.1X statistics for all the specified ports. If no ports are specified, the command clears all 802.1X statistics.

Related commands: **display dot1x**.

Examples

# Clear 802.1X statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

EAD fast deployment configuration commands

dot1x free-ip

Syntax

dot1x free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x free-ip { *ip-address* { *mask* | *mask-length* } | **all** }

View

System view

Default level

2: System level

Parameters

ip-address: Specifies a freely accessible IP address segment, also called "a free IP."

mask: Specifies an IP address mask.

mask-length: Specifies IP address mask length.

all: Removes all free IP addresses.

Description

Use **dot1x free-ip** to configure a free IP. Users can access the segment before passing 802.1X authentication.

Use **undo dot1x free-ip** to remove the specified or all free IP addresses.

By default, no free IP is configured.

When global MAC authentication, Layer-2 portal authentication, or port security is enabled, the free IP does not take effect.

Related commands: **display dot1x**.

Examples

# Configure 192.168.0.0/24 as a free IP address.

```
<Sysname> system-view
[Sysname] dot1x free-ip 192.168.0.0 24
```

dot1x timer ead-timeout

Syntax

dot1x timer ead-timeout *ead-timeout-value*

undo dot1x timer ead-timeout

View

System view

Default level

2: System level

Parameters

ead-timeout-value: Specifies the EAD rule timer in minutes, in the range of 1 to 1440.

Description

Use **dot1x timer ead-timeout** to set the EAD rule timer.

Use **undo dot1x timer ead-timeout** to restore the default.

By default, the timer is 30 minutes.

EAD fast deployment automatically creates an ACL rule, or EAD rule, to open access to the redirect URL for each redirected user seeking to access the network. The EAD rule timer sets the lifetime of each ACL rule. When the timer expires or the user passes authentication, the rule is removed. If users fail to download EAD client or pass authentication before the timer expires, they must reconnect to the network to access the free IP.

To prevent ACL rule resources from being used up, you can shorten the timer when the amount of EAD users is large.

Related commands: **display dot1x**.

Examples

# Set the EAD rule timer to 5 minutes.

```
<Sysname> system-view
[Sysname] dot1x timer ead-timeout 5
```

dot1x url

Syntax

dot1x url *url-string*

undo dot1x url

View

System view

Default level

2: System level

Parameters

url-string: Specifies the redirect URL, a case-sensitive string of 1 to 64 characters in the format http://string.

Description

Use **dot1x url** to configure a redirect URL. When a user uses a web browser to access networks other than the free IP, the device redirects the user to the redirect URL.

Use **undo dot1x url** to remove the redirect URL.

By default, no redirect URL is defined.

The redirect URL must be on the free IP subnet.

If you configure the **dot1x url** command multiple times, the last configured URL takes effect.

Related commands: **display dot1x** and **dot1x free-ip**.

Examples

# Configure the redirect URL as http://192.168.0.1.

```
<Sysname> system-view
[Sysname] dot1x url http://192.168.0.1
```

MAC authentication configuration commands

display mac-authentication

Syntax

display mac-authentication [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-authentication** to display MAC authentication settings and statistics, including the global settings, and port-specific settings and MAC authentication and online user statistics.

If you specify a list of ports, the command displays port-specific settings and statistics only for the specified ports.

If you do not specify any port, the command displays port-specific settings and statistics for all ports.

Examples

# Display all MAC authentication settings and statistics.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 300s
          Quiet period is 60s.
          Server response timeout value is 100s
          the max allowed user number is 1024 per slot
          Current user number amounts to 0
          Current domain: not configured, use default domain

Silent Mac User info:
         MAC Addr         From Port           Port Index
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 0, failed: 0
 Max number of on-line users is 256
  Current online user number is 0
MAC Addr         Authenticate state           AuthIndex
…
```

Table 11 Command output

Field	Description
MAC address authentication is enabled	Whether MAC authentication is enabled
User name format is MAC address in lowercase, like xxxxxxxxxxxx	Type of user account, which can be MAC-based or shared. • If MAC-based accounts are used, this field displays "User name format is MAC address…" and the format settings for usernames and passwords. For example, MAC addresses without hyphens in lower case. • If a shared account is used, this field displays "User name format is fixed account."
Fixed username:	Username of the shared account for MAC authentication users. If MAC-based accounts are used, this field displays **mac**.
Fixed password:	Password of the shared account for MAC authentication users. If MAC-based accounts are used, this field displays **not configured**.
Offline detect period	Setting of the offline detect timer
Quiet period	Setting of the quiet timer
Server response timeout value	Setting of the server timeout timer
the max allowed user number	Maximum number of users each slot supports
Current user number amounts to	Number of online users
Current domain: not configured, use default domain	Authentication domain that is currently used
Silent Mac User info	Information about silent MAC addresses. A MAC address is marked silent when it fails a MAC authentication, and at the same time, a quiet timer starts. Before the timer expires, the device drops any packet from the MAC address and does not perform MAC authentication for the MAC address.
GigabitEthernet 1/0/1 is link-up	Status of the link on port GigabitEthernet 1/0/1. In this example, the link is up.
MAC address authentication is enabled	Whether MAC authentication is enabled on port GigabitEthernet1/0/1.
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful and unsuccessful authentication attempts

Field	Description
Max number of on-line users	Maximum number of concurrent online users allowed on the port. If MAC authentication is not enabled on the port, the field displays **0**.
Current online user number	Number of online users on the port.
MAC Addr	MAC address of the online user.
Authenticate state	User status: • **MAC_AUTHENTICATOR_CONNECT**—The user is logging in. • **MAC_AUTHENTICATOR_SUCCESS**—The user has passed the authentication. • **MAC_AUTHENTICATOR_FAIL**—The user failed the authentication. • **MAC_AUTHENTICATOR_LOGOFF**—The user has logged off.
AuthIndex	Authenticator index.

mac-authentication

Syntax

In system view:

mac-authentication [**interface** *interface-list*]

undo mac-authentication [**interface** *interface-list*]

In Ethernet interface view:

mac-authentication

undo mac-authentication

View

System view, Ethernet interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description

Use **mac-authentication** in system view to enable MAC authentication globally.

Use **mac-authentication interface** *interface-list* in system view to enable MAC authentication on a list of ports, or **mac-authentication** in interface view to enable MAC authentication on a port.

Use **undo mac-authentication** in system view to disable MAC authentication globally.

Use **undo mac-authentication interface** *interface-list* in system view to disable MAC authentication on a list of ports, or **undo mac-authentication** in interface view to disable MAC authentication on a port.

By default, MAC authentication is not enabled globally or on any port.

To use MAC authentication on a port, you must enable the function both globally and on the port.

Examples

# Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

# Enable MAC authentication on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

mac-authentication critical vlan

Syntax

mac-authentication critical vlan *critical-vlan-id*

undo mac-authentication critical vlan

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

critical-vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Description

Use **mac-authentication critical vlan** to configure a MAC authentication critical VLAN on a port for MAC authentication users that have failed authentication because all the RADIUS authentication servers in their ISP domain are unreachable.

Use **undo mac-authentication critical vlan** to restore the default.

By default, no MAC authentication critical VLAN is configured on a port.

The MAC authentication critical VLAN configuration applies to MAC authentication users that use only RADIUS authentication servers and have failed authentication because all the servers in their ISP domain become unavailable (inactive), for example, for the loss of network connectivity. If a MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

You can configure only one MAC authentication critical VLAN on a port. The MAC authentication critical VLANs on different ports can be different.

To have the MAC authentication critical VLAN take effect on a port, complete the following tasks:

- Enable MAC authentication both globally and on the port.
- Enable MAC-based VLAN on the port.

To delete a VLAN that has been configured as a MAC authentication critical VLAN, you must remove the MAC authentication critical VLAN configuration first.

Related commands: **mac-authentication**; **mac-vlan enable** (the *Layer 2—LAN Switching Command Reference*).

Examples

# Specify VLAN 5 as the MAC authentication critical VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 5
```

mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

View

System view, Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies an authentication domain name, a case-insensitive string of 1 to 24 characters. The domain name cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or at sign (@).

Description

Use **mac-authentication domain** to specify a global authentication domain in system view or a port specific authentication domain in interface view for MAC authentication users.

Use **undo mac-authentication domain** to restore the default.

By default, the default authentication domain is used for MAC authentication users. For more information about the default authentication domain, see the **domain default enable** command in "AAA configuration commands."

The global authentication domain is applicable to all MAC authentication enabled ports. A port specific authentication domain is applicable only to the port. You can specify different authentication domains on different ports.

A port chooses an authentication domain for MAC authentication users in this order: port specific domain, global domain, and the default authentication domain.

Related commands: **display mac-authentication**.

Examples

# Specify the **domain1** domain as the global authentication domain for MAC authentication users.

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

# Specify the **aabbcc** domain as the authentication domain for MAC authentication users on port GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

mac-authentication guest-vlan

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

View

Ethernet interface view

Default level

2: System level

Parameters

guest-vlan-id: Specifies a VLAN as the MAC authentication guest VLAN. The value range is from 1 to 4094. Make sure that the VLAN has been created.

Description

Use **mac-authentication guest-vlan** to specify a MAC authentication guest VLAN on a port. Any users that have failed MAC authentication on the port is assigned to this VLAN, so they can access a limited set of network resources, such as a software server, to download anti-virus software, and system patches. After a user in the guest VLAN passes MAC authentication, it is removed from the guest VLAN and can access all authorized network resources.

Use **undo mac-authentication guest-vlan** to remove the MAC authentication guest VLAN from the port.

By default, no MAC authentication guest VLAN is configured on a port.

To use the MAC authentication guest VLAN function on a port, you must enable MAC-based VLAN on the port, in addition to enabling MAC authentication both globally and on the port.

To delete a VLAN that has been set as a MAC authentication guest VLAN, remove the guest VLAN configuration first.

Related commands: **mac-authentication**; **mac-vlan enable** (the *Layer 2—LAN Switching Command Reference*).

Examples

# Configure VLAN 5 as the MAC authentication guest VLAN on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 5
```

mac-authentication max-user

Syntax

mac-authentication max-user *user-number*

undo mac-authentication max-user

View

Ethernet interface view

Default level

2: System level

Parameters

user-number: Specifies a maximum number of concurrent MAC authentication users on the port. The value is in the range of 1 to 256.

Parameters

Use **mac-authentication max-user** to set the maximum number of concurrent MAC authentication users on a port.

Use **undo mac-authentication max-user** to restore the default.

By default, maximum number of concurrent MAC authentication users on a port is 256.

Examples

# Configure port GigabitEthernet 1/0/1 to support up to 32 concurrent MAC authentication users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View

System view

Default level

2: System level

Parameters

offline-detect *offline-detect-value*: Sets the offline detect timer, in the range of 60 to 65535 seconds. This timer sets the interval that the device waits for traffic from a user before it regards the user idle. If a user connection has been idle for two consecutive intervals, the device logs the user out and stops accounting for the user.

quiet *quiet-value*: Sets the quiet timer, in the range of 1 to 3600 seconds. This timer sets the interval that the device must wait before it can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds, in the range of 100 to 300. This timer sets the interval that the access device waits for a response from a RADIUS server before it regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Description

Use **mac-authentication timer** to set the MAC authentication timers.

Use **undo mac-authentication timer** to restore the defaults.

By default, the offline detect timer is 300 seconds, the quiet timer is 60 seconds, and the server timeout timer is 100 seconds.

Related commands: **display mac-authentication**.

Examples

# Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

View

System view

Default level

2: System level

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name takes a case-insensitive string of 1 to 55 characters. If no username is specified, the default name **mac** applies.

password: Specifies the password for the shared user account.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password. This argument is case sensitive. If **simple** is specified, the password must be a string of 1 to 63 characters. If **cipher** is specified, the password must be a ciphertext string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. If this option is specified, you must create one user account for each user, and use the MAC address of the user as both the username and password for the account. You can also specify the format of username and password:

- **with-hyphen**—Hyphenates the MAC address, for example xx-xx-xx-xx-xx-xx.
- **without-hyphen**—Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx.
- **lowercase**—Enters letters in lower case.
- **uppercase**—Capitalizes letters.

Description

Use **mac-authentication user-name-format** to configure the type of user accounts for MAC authentication users.

Use **undo mac-authentication user-name-format** to restore the default.

By default, each user's MAC address is used as the username and password for MAC authentication, and letters must be input in lower case without hyphens.

MAC authentication supports the following types of user account:

- One MAC-based user account for each user. A user can pass MAC authentication only when its MAC address matches a MAC-based user account. This approach is suitable for an insecure environment.
- One shared user account for all users. Any user can pass MAC authentication on any MAC authentication enabled port. You can use this approach in a secure environment to limit network resources accessible to MAC authentication users, for example, by assigning an authorized ACL or VLAN for the shared account.

The configuration file saves the password for a shared user account in cipher text, regardless of whether it is specified in cipher text or plain text.

Related commands: **display mac-authentication**.

Examples

# Configure a shared account for MAC authentication users: set the username as **abc** and password as **xyz** in plain text.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

# Configure a shared account for MAC authentication users: set the username as **abc** and password as a ciphertext string of **$c$3$Uu9Dh4xRKWa8RHW3TFnNTafBbhdPAg**.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password cipher
$c$3$Uu9Dh4xRKWa8RHW3TFnNTafBbhdPAg
```

# Use MAC-based user accounts for MAC authentication users, and each MAC address must be hyphenated, and in upper case.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address with-hyphen uppercase
```

reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**interface** *interface-list*]

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description

Use **reset mac-authentication statistics** to clear MAC authentication statistics.

If no port list is specified, the command clears all global and port-specific MAC authentication statistics. If a port list is specified, the command clears the MAC authentication statistics on the specified ports.

Related commands: **display mac-authentication**.

Examples

# Clear MAC authentication statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

Portal configuration commands

display portal free-rule

Syntax

display portal free-rule [*rule-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

rule-number: Specifies the number of a portal-free rule. The value range is from 0 to 255.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal free-rule** to display information about a specified portal-free rule or all portal-free rules.

Related commands: **portal free-rule**.

Examples

# Display information about portal-free rule 1.

```
<Sysname> display portal free-rule 1
 Rule-Number  1:
 Source:
   IP        : 2.2.2.0
   Mask      : 255.255.255.0
   MAC       : 0000-0000-0000
   Interface : any
   Vlan      : 0
 Destination:
   IP        : 0.0.0.0
   Mask      : 0.0.0.0
```

Table 12 Command output

Field	Description
Rule-Number	Number of the portal-free rule

Field	Description
Source	Source information in the portal-free rule
IP	Source IP address in the portal-free rule
Mask	Subnet mask of the source IP address in the portal-free rule
MAC	Source MAC address in the portal-free rule
Interface	Source interface in the portal-free rule
Vlan	Source VLAN in the portal-free rule
Destination	Destination information in the portal-free rule
IP	Destination IP address in the portal-free rule
Mask	Subnet mask of the destination IP address in the portal-free rule

display portal interface

Syntax

display portal interface *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal interface** to display the portal configuration of an interface.

Examples

# Display the portal configuration of interface GigabitEthernet1/0/1.

```
<Sysname> display portal interface gigabitethernet1/0/1
 Interface portal configuration:
 GigabitEthernet1/0/1: Portal running
 Portal server: servername
Authentication type: Direct
 Authentication domain: my-domain
 Authentication network:
```

```
 source address : 0.0.0.0  mask : 0.0.0.0
 destination address : 2.2.2.0.  mask : 255.255.255.0
```

Table 13 Command output

Field	Description
Interface portal configuration	Portal configuration on the interface
GigabitEthernet1/0/1	Status of the portal authentication on the interface: • **disabled**—Portal authentication is disabled. • **enabled**—Portal authentication is enabled but is not functioning. • **running**—Portal authentication is functioning.
Portal server	Portal server referenced by the interface
Authentication type	Authentication mode enabled on the interface
Authentication domain	Mandatory authentication domain of the interface
Authentication network	Information of the portal authentication source subnet and destination subnet.
address	IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

display portal local-server

Syntax

display portal local-server [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal local-server** to display configuration information about the local portal server, including the supported protocol type, and the referenced SSL server policy.

Related commands: **portal local-server** and **portal local-server bind**.

Examples

# Display configuration information about the local portal server.

```
<Sysname> display portal local-server
```

```
 Protocol:
 Local-server IP: 255.255.255.255
 Server policy:
```

Table 14 Command output

Field	Description
Protocol	Protocol supported by the local portal server, HTTP or HTTPS.
Server policy	SSL server policy associated with the HTTPS service. If HTTP is configured, this field is empty.

display portal tcp-cheat statistics

Syntax

display portal tcp-cheat statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal tcp-cheat statistics** to display TCP spoofing statistics.

Examples

# Display TCP spoofing statistics.

```
<Sysname> display portal tcp-cheat statistics
 TCP Cheat Statistic:
 Total Opens: 0
 Resets Connections: 0
 Current Opens: 0
 Packets Received: 0
 Packets Sent: 0
 Packets Retransmitted: 0
 Packets Dropped: 0
 HTTP Packets Sent: 0
 Connection State:
          SYN_RECVD: 0
          ESTABLISHED: 0
```

```
CLOSE_WAIT: 0
LAST_ACK: 0
FIN_WAIT_1: 0
FIN_WAIT_2: 0
CLOSING: 0
```

Table 15 Command output

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections
Resets Connections	Number of connections reset through RST packets
Current Opens	Number of connections being set up
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of HTTP packets sent
Connection State	Statistics of connections in various states
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

display portal user

Syntax

display portal user { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Specifies all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and name.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal user** to display information about portal users on a specified interface or all interfaces.

Examples

# Display information about portal users on all interfaces.

```
<Sysname> display portal user all
 Index:2
 State:ONLINE
 SubState:NONE
 ACL:NONE
 Work-mode:Stand-alone
 MAC                IP                 Vlan   Interface
 ---------------------------------------------------------------------
 000d-88f8-0eab   2.2.2.2           1      GigabitEthernet1/0/1
Total 1 user(s) matched, 1 listed..
```

Table 16 Command output

Field	Description
Index	Index of the portal user
State	Current status of the portal user
SubState	Current sub-status of the portal user
ACL	Authorization ACL of the portal user
Work-mode	User's working mode: - Primary - Secondary - Stand-alone
MAC	MAC address of the portal user
IP	IP address of the portal user
Vlan	VLAN to which the portal user belongs
Interface	Interface to which the portal user is attached
Total 1 user(s) matched, 1 listed	Total number of portal users

portal auth-fail vlan

Syntax

portal auth-fail vlan *authfail-vlan-id*

undo portal auth-fail vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

authfail-vlan-id: Specifies the Auth-Fail VLAN ID. After an Auth-Fail VLAN is specified, a client failing portal authentication will be added to the Auth-Fail VLAN.

Description

Use **portal auth-fail vlan** to specify an Auth-Fail VLAN for portal authentication on the current port.

Use **undo portal auth-fail vlan** to restore the default setting.

By default, no Auth-Fail VLAN is specified for portal authentication on a port.

The specified VLAN must exist.

To make the Auth-Fail VLAN take effect, you need to enable the MAC VLAN function on the port.

You can specify different Auth-Fail VLANs for portal authentication on different ports. A port can be specified with only one Auth-Fail VLAN for portal authentication.

Examples

# Configure VLAN 5 as the Auth-VLAN of portal authentication on port GigabitEthernet 1/0/1, so that the port will add users failing portal authentication to this VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] mac-vlan enable
[Sysname-GigabitEthernet1/0/1] portal auth-fail vlan 5
```

portal delete-user

Syntax

portal delete-user { *ip-address* | **all** | **interface** *interface-type interface-number* }

View

System view

Default level

2: System level

Parameters

ip-address: Logs off the user with the specified IP address.

all: Logs off all users.

interface *interface-type interface-number*: Logs off all users on the specified interface.

Description

Use **portal delete-user** to log off users.

Related commands: **display portal user**.

Examples

# Log out the user whose IP address is 1.1.1.1.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

portal domain

Syntax

portal domain *domain-name*

undo portal domain

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters. The domain specified by this argument must already exist.

Description

Use **portal domain** to specify an authentication domain for an interface. Then, the device will use the authentication domain for authentication, authorization and accounting (AAA) of the portal users on the interface.

Use **undo portal domain** to restore the default.

By default, no authentication domain is specified for portal users on an interface.

Related commands: **display portal interface**.

Examples

# Configure the authentication domain to be used for IPv4 portal users on port GigabitEthernet 1/0/1 as **my-domain**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-Gigabitethernet1/0/1] portal domain my-domain
```

portal free-rule

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } | **source any** } *

undo portal free-rule { *rule-number* | **all** }

View

System view

Default level

2: System level

Parameters

rule-number: Specifies a number for the portal-free rule, in the range 0 to 255.

any: Imposes no limitation on the previous keyword.

ip *ip-address*: Specifies an IP address.

mask { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range of 0 to 32.

all: Specifies all portal-free rules.

Description

Use **portal free-rule** to configure a portal-free rule and specify the source filtering condition, destination filtering condition, or both.

Use **undo portal free-rule** to remove a specified portal-free rule or all portal-free rules.

If you specify both the source IPv4 address and source MAC address, the IPv4 address must be a host address with a 32-bit mask. Otherwise, the specified MAC address does not take effect.

You cannot configure a portal-free rule to have the same filtering criteria as that of an existing one. When attempted, the system prompts that the rule already exists.

You can only add or remove a portal-free rule. You cannot modify it.

For Layer 2 portal authentication, you can configure only portal-free rules that are from any source address to any or a specific destination address. With such a portal-free rule configured, users can access the specified address without portal authentication.

Related commands: **display portal free-rule**.

Examples

# Configure a portal-free rule, allowing packets destined for 10.10.10.1/24 to bypass portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 16 destination ip 10.10.10.1 mask 24 source any
```

portal local-server

Syntax

portal local-server { **http** | **https server-policy** *policy-name* }

undo portal local-server { **http** | **https** }

View

System view

Default level

2: System level

Parameters

http: Specifies that the local portal server use HTTP to exchange authentication packets with clients.

https: Specifies that the local portal server use HTTPS to exchange authentication packets with clients.

server-policy *policy-name*: Specifies the SSL server policy to be associated with the HTTPS service. *policy-name* indicates an SSL server policy name, a case-insensitive string of 1 to 16 characters.

Description

Use **portal local-server** to configure the protocol type to be supported by the local portal server and load the default authentication page file.

Use **undo portal local-server** to cancel the configuration.

By default, the local portal server does not support any protocol type.

When executing this command, the local portal server will load the default authentication page file, which is supposed to be saved in the root directory of the device. To ensure that the local portal server uses the user-defined default authentication pages, edit and save them properly before executing this command. Otherwise, the system default authentication pages will be used.

If you specify HTTP in this command, the redirection URL for HTTP packets is in the format of http://*IP address of the device*/portal/logon.htm, and clients and the portal server exchange authentication information through HTTP.

If you specify HTTPS in this command, the redirection URL for HTTP packets is in the format of https://*IP address of the device*/portal/logon.htm, and clients and the portal server exchange authentication information through HTTPS.

You cannot remove an SSL server policy using the **undo ssl server-policy** command if the policy has been referenced by the HTTPS service.

On the device, all the SSL server policies referenced by the HTTPS service must be the same.

If an online portal user exists on the device, you cannot remove or change the configured protocol type, or modify the SSL server policies referenced.

To change the SSL server policy referenced by HTTPS service, you must cancel the HTTPS configuration using the **undo portal local-server https** command, and then specify the desired SSL server policy.

Related commands: **display portal local-server** and **ssl server-policy**.

Examples

# Configure the local portal server to support HTTP.

```
<Sysname> system-view
[Sysname] portal local-server http
```

# Configure the local portal server to support HTTPS and reference SSL server policy **policy1**, which has been configured already.

```
<Sysname> system-view
[Sysname] portal local-server https server-policy policy1
```

# Change the referenced SSL server policy to **policy2**.

```
[Sysname] undo portal local-server https
[Sysname] portal local-server https server-policy policy2
```

portal local-server enable

Syntax

portal local-server enable

undo portal

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **portal local-server enable** to enable Layer 2 portal authentication on the current port.

Use **undo portal** to restore the default.

By default, portal authentication is disabled on a Layer 2 port.

For normal operation of portal authentication on a Layer 2 port, and HP recommends disabling port security, guest VLAN of 802.1X, and EAD fast deployment of 802.1X on the port. For information about port security and 802.1X features, see *Security Configuration Guide*.

Before enabling portal authentication on a Layer 2 port, be sure to specify the listening IP address of the local portal server.

Related command: **portal local-server ip**.

Examples

# Enable Layer 2 portal authentication on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal local-server enable
```

portal local-server ip

Syntax

portal local-server ip *ip-address*

undo portal local-server ip

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the listening IP address of the local portal server. This IP address is that of a Layer 3 interface on the access device and can reach the portal client.

Description

Use **portal local-server ip** to specify the listening IP address of the local portal server for Layer 2 portal authentication. With a listening IP address specified, the device will redirect Web requests from portal clients to the authentication page at the listening IP address.

Use **undo portal local-server ip** to restore the default.

By default, no listening IP address is specified for the local portal server.

HP recommends configuring a loopback interface's address as the listening IP address because:

- The status of a loopback interface is stable. This can avoid authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets. This can avoid impacting system performance when there are many network access requests.

Examples

# Specify 1.1.1.1 as the listening IP address of the local portal server for Layer 2 portal authentication.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] ip address 1.1.1.1 32
[Sysname-LoopBack1] quit
[Sysname] portal local-server ip 1.1.1.1
```

portal max-user

Syntax

portal max-user *max-number*

undo portal max-user

View

System view

Default level

2: System level

Parameters

max-number: Specifies the maximum number of online portal users allowed in the system. The value is in the range of 1 to 1000.

Description

Use **portal max-user** to set the maximum number of online portal users allowed in the system.

Use **undo portal max-user** to restore the default.

By default, the maximum number of portal users allowed on the switch is 1000.

If the maximum number of portal users specified in the command is less than that of the current online portal users, the command can be executed successfully and will not impact the online portal users, but the system will not allow new portal users to log in until the number drops down below the limit.

Examples

# Set the maximum number of portal users allowed in the system to 100.

```
<Sysname> system-view
[Sysname] portal max-user 100
```

portal move-mode auto

Syntax

portal move-mode auto

undo portal move-mode

View

System view

Default level

2: System level

Parameters

None

Description

Use **portal move-mode auto** to enable support for portal user moving. Then, if an authenticated user moves from a port of the device to another port of the device without logging off, the user can continue to access the network (without re-authentication) if the following conditions are satisfied:

- The new port is up.
- The original port and the new port belong to the same VLAN.
- The authorization information of the user, if any, is assigned to the new port successfully.

If any condition is not satisfied, the device re-authenticates the user on the new port.

Use **undo portal move-mode** to disable support for portal user moving.

By default, support for portal user moving is disabled, and if an authenticated user moves from a port of the device to another port of the device without logging off, the user cannot get online when the original port is still up, because the original port is still maintaining the authentication information of the user.

If the original port goes down after a user moves from the port to another port, the authentication information of the user is lost and the user has to be re-authenticated.

Support for portal user moving applies to scenarios where hubs, Layer 2 switches, or APs exist between users and the access devices.

Examples

# Enable support for portal user moving.

```
<Sysname> system-view
[Sysname] portal move-mode auto
```

portal offline-detect interval

Syntax

portal offline-detect interval *offline-detect-interval*

undo portal offline-detect interval

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

offline-detect-value: Specifies the online Layer 2 portal user detection interval, in the range of 60 to 65535.

Description

Use **portal offline-detect interval** to set the online Layer 2 portal user detection interval. Then, after a Layer 2 portal user gets online, the device starts a detection timer for the user, and checks whether the user has sent any packet to the device at this interval. If the device receives no packets from the user during two detection intervals or finds that the user's MAC address entry has been aged out, the device considers that the user has gone offline and clears the authentication information of the user.

Use **undo portal offline-detect interval** to restore the default.

By default, the online Layer 2 portal user detection interval is 300 seconds.

This detection interval must be equal to or less than the MAC address entry aging time. Otherwise, many portal users will be considered offline due to aged MAC address entries.

Examples

# Set the online Layer 2 portal user detection interval to 3600 seconds on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal offline-detect interval 3600
```

portal redirect-url

Syntax

portal redirect-url *url-string* [**wait-time** *period*]

undo portal redirect-url

View

System view

Default level

2: System level

Parameters

url-string: Specifies an auto redirection URL for authenticated portal users, a string of 1 to 127 characters. It must start with http:// or https:// and must be a fully qualified URL.

wait-time *period*: Specifies the time that the device must wait before redirecting a user passing portal authentication to the auto redirection URL. It ranges from 1 to 90 and defaults to 5, in seconds.

Description

Use **portal redirect-url** to specify the auto redirection URL for authenticated portal users.

Use **undo portal redirect-url** to restore the default.

By default, a user authenticated is redirected to the URL the user typed in the address bar before portal authentication.

The **wait-time** *period* option is effective to only local portal authentication.

If a Layer 2 portal user is to be assigned a VLAN after passing portal authentication, the user may need to update the IP address after getting online. In this case, the redirection wait time must be longer than the user IP address update time. Otherwise, the user may not be able to open the URL because the expected IP address update is not complete yet.

Examples

# Configure the device to redirect a portal user to **http://www.testpt.cn** 3 seconds after the user passes portal authentication.

```
<Sysname> system-view
[Sysname] portal redirect-url http://www.testpt.cn wait-time 3
```

portal server banner

Syntax

portal server banner *banner-string*

undo portal server banner

View

System view

Default level

2: System level

Parameters

banner-string: Specifies a welcome banner for the Web page, a case-sensitive string of 1 to 50 characters. It cannot contain the less-than sign (<) or the and sign (&). If multiple continuous spaces exist in the string, the browser will recognize them as one.

Description

Use **portal server banner** to configure the welcome banner of the default Web page provided by the local portal server.

Use **undo portal server banner** to restore the default.

By default, no Web page welcome banner is configured.

The configured welcome banner is applied to only the default authentication pages, rather than the customized authentication pages.

Examples

# Configure the welcome banner of the default Web page provided by the local portal server as **Welcome to Portal Authentication**.

```
<Sysname> system-view
[Sysname] portal server banner Welcome to Portal Authentication
```

portal web-proxy port

Syntax

portal web-proxy port *port-number*

undo portal web-proxy port { **all** | *port-number* }

View

System view

Default level

2: System level

Parameters

all: Specifies all web proxy server port numbers.

port-number: Specifies the port number used by a web proxy server, in the range of 1 to 65535.

Description

Use **portal web-proxy port** to add the port number of a web proxy server, so that HTTP requests forwarded by the web proxy server trigger portal authentication.

Use **undo portal web-proxy port** to delete one or all web proxy server port numbers.

By default, no web proxy server port number is configured on the device and proxied HTTP requests cannot trigger portal authentication.

Only layer 2 portal authentication supports this function.

Up to four web proxy server port numbers can be added.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover web proxy servers, you must add the port numbers of the web proxy servers on the device, and configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

You must add the port numbers of the web proxy servers on the device, and users must ensure that their browsers that use a web proxy server do not use the proxy server for the listening IP address of the local portal server. Thus, HTTP packets that the portal user sends to the local portal server are not sent to the web proxy server.

Examples

# Add web proxy server port number 8080 on the device, so that users using a web proxy server with the port number can be redirected to the portal authentication page.

```
<Sysname> system-view
[Sysname] portal web-proxy port 8080
```

reset portal tcp-cheat statistics

Syntax

reset portal tcp-cheat statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset portal tcp-cheat statistics** to clear TCP spoofing statistics.

Examples

# Clear TCP spoofing statistics.

```
<Sysname> reset portal tcp-cheat statistics
```

Port security configuration commands

display port-security

Syntax

display port-security [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-list*: Specifies Ethernet ports by an Ethernet port list in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 ports or port ranges. The starting port and ending port of a port range must be of the same type, and the ending port number must be greater than the starting port number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security** to display port security configuration information, operation information, and statistics for one or more ports.

If the **interface** *interface-list* parameter is not provided, the command displays port security information, operation information, and status about all ports.

Related commands: **port-security enable**, **port-security port-mode**, **port-security ntk-mode**, **port-security intrusion-mode**, **port-security max-mac-count**, **port-security mac-address security**, **port-security authorization ignore**, **port-security oui**, and **port-security trap**.

Examples

# Display port security configuration information, operation information, and statistics for all ports.

```
<Sysname> display port-security
 Equipment port-security is enabled
 AddressLearn trap is enabled
 Intrusion trap is enabled
 Dot1x logon trap is enabled
 Dot1x logoff trap is enabled
 Dot1x logfailure trap is enabled
 RALM logon trap is enabled
 RALM logoff trap is enabled
 RALM logfailure trap is enabled
 AutoLearn aging time is 1 minutes
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 000d1a
   Index is 2,  OUI value is 003c12

GigabitEthernet1/0/1 is link-down
    Port mode is userLoginWithOUI
    NeedToKnow mode is NeedToKnowOnly
    Intrusion Portection mode is DisablePort
    Max MAC address number is 50
    Stored MAC address number is 0
    Authorization is ignored
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
 GigabitEthernet1/0/2 is link-down
    Port mode is noRestriction
    NeedToKnow mode is disabled
    Intrusion mode is NoAction
    Max MAC address number is not configured
    Stored MAC address number is 0
    Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

Table 17 Command output

Field	Description
Equipment port-security	Whether the port security is enabled or not.
AddressLearn trap	Whether trapping for MAC address learning is enabled or not. If it is enabled, the port sends trap information after it learns a new MAC address.
Intrusion trap	Whether trapping for intrusion protection is enabled or not. If it is enabled, the port sends trap information after it detects illegal packets.
Dot1x logon trap	Whether trapping for 802.1X logon is enabled or not. If it is enabled, the port sends trap information after a user passes 802.1X authentication.
Dot1x logoff trap	Whether trapping for 802.1X logoff is enabled or not. If it is enabled, the port sends trap information after an 802.1X user logs off.
Dot1x logfailure	Whether trapping for 802.1X authentication failure is enabled or not. If it is enabled, the port sends trap information after a user fails 802.1X authentication.
RALM logon trap	Whether trapping for MAC authentication success is enabled or not. If it is enabled, the port sends trap information when a user passes MAC address authentication.
RALM logoff trap	Whether trapping for MAC authenticated user logoff is enabled or not. If it is enabled, traps are sent when a MAC address authenticated user logs off.

Field	Description
RALM logfailure trap	Whether trapping for MAC authentication failure is enabled or not. If it is enabled, the port sends trap information when a user fails MAC address authentication.
AutoLearn aging time	Secure MAC aging timer. The timer applies to sticky or dynamic secure MAC addresses.
Disableport Timeout	Silence timeout period of the port that receives illegal packets, in seconds.
OUI value	List of OUI values allowed
Port mode	Port security mode: • noRestrictions • autoLearn • macAddressWithRadius • macAddressElseUserLoginSecure • macAddressElseUserLoginSecureExt • secure • userLogin • userLoginSecure • userLoginSecureExt • macAddressOrUserLoginSecure • macAddressOrUserLoginSecureExt • userLoginWithOUI
NeedToKnow mode	Need to know (NTK) mode: • **NeedToKnowOnly**—Allows only unicast packets with authenticated destination MAC addresses. • **NeedToKnowWithBroadcast**—Allows only unicast packets and broadcasts with authenticated destination MAC addresses. • **NeedToKnowWithMulticast**—Allows unicast packets, multicasts and broadcasts with authenticated destination MAC addresses.
Intrusion mode	Intrusion protection action mode: • **BlockMacAddress**—Adds the source MAC address of the illegal packet to the blocked MAC address list. • **DisablePort**—Shuts down the port that receives illegal packets permanently. • **DisablePortTemporarily**—Shuts down the port that receives illegal packets for some time. • **NoAction**—Performs no intrusion protection.
Max MAC address number	Maximum number of MAC addresses that port security allows on the port.
Stored MAC address number	Number of MAC addresses stored
Authorization	Whether the authorization information from the server is ignored or not: • **permitted**—Authorization information from the RADIUS server takes effect. • **ignored**—Authorization information from the RADIUS server does not take effect.

display port-security mac-address block

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security mac-address block** to display information about blocked MAC addresses.

With no keyword or argument specified, the command displays information about all blocked MAC addresses.

Related commands: **port-security intrusion-mode**.

Examples

# Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
MAC ADDR              From Port                            VLAN ID

 --- On slot 0, no mac address found ---
000f-3d80-0d2d       GigabitEthernet1/0/1                30

--- On slot 1, 1 mac address(es) found ---
--- 1 mac address(es) found ---
```

# Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count

--- On slot 0, no mac address found ---

--- On slot 1, 1 mac address(es) found ---
--- 1 mac address(es) found ---
```

# Display information about all blocked MAC addresses in VLAN 30.

```
<Sysname> display port-security mac-address block vlan 30
MAC ADDR             From Port                             VLAN ID

 --- On slot 0, no mac address found ---
000f-3d80-0d2d       GigabitEthernet1/0/1               30

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
```

# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1.

```
<Sysname> display port-security mac-address block interface gigabitethernet1/0/1
MAC ADDR             From Port                           VLAN ID
000f-3d80-0d2d      GigabitEthernet1/0/1               30

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
```

# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1 in VLAN 30.

```
<Sysname> display port-security mac-address block interface gigabitethernet 1/0/1 vlan
30
MAC ADDR             From Port                          VLAN ID

000f-3d80-0d2d       GigabitEthernet1/0/1               30
--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
```

Table 18 Command output

Field	Description
MAC ADDR	Blocked MAC address
From Port	Port having received frames with the blocked MAC address being the source address
VLAN ID	ID of the VLAN to which the port belongs
x mac address(es) found	Number of blocked MAC addresses

display port-security mac-address security

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

count: Displays only the count of the secure MAC addresses.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security mac-address security** to display information about secure MAC addresses. Secure MAC addresses are those that are automatically learned by the port in autoLearn mode or configured by the **port-security mac-address security** command.

With no keyword or argument specified, the command displays information about all secure MAC addresses.

Related commands: **port-security mac-address security**.

Examples

# Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
MAC ADDR       VLAN ID   STATE         PORT INDEX                      AGING TIME(s)
0002-0002-0002  1         Security      GigabitEthernet1/0/1             NOAGED
000d-88f8-0577  1         Security      GigabitEthernet1/0/1             NOAGED

  ---  2 mac address(es) found  ---
```

# Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address security count
 2 mac address(es) found
```

# Display information about secure MAC addresses in VLAN 1.

```
<Sysname> display port-security mac-address security vlan 1
MAC ADDR       VLAN ID   STATE         PORT INDEX                      AGING TIME(s)
0002-0002-0002  1         Security      GigabitEthernet1/0/1             NOAGED
000d-88f8-0577  1         Security      GigabitEthernet1/0/1             NOAGED

  ---  2 mac address(es) found  ---
```

# Display information about secure MAC addresses on port GigabitEthernet 1/0/1.

```
<Sysname> display port-security mac-address security interface gigabitethernet1/0/1
MAC ADDR       VLAN ID   STATE         PORT INDEX                      AGING TIME(s)
000d-88f8-0577  1         Security     GigabitEthernet1/0/1             NOAGED
```

```
  ---  1 mac address(es) found  ---
```

# Display information about secure MAC addresses of port GigabitEthernet 1/0/1 in VLAN 1.

```
<Sysname> display port-security mac-address security interface gigabitethernet 1/0/1 vlan
1
MAC ADDR        VLAN ID   STATE          PORT INDEX                          AGING TIME(s)
000d-88f8-0577  1          Security       GigabitEthernet1/0/1                 NOAGED

  ---  1 mac address(es) found  ---
```

Table 19 Command output

Field	Description
MAC ADDR	Secure MAC address
VLAN ID	ID of the VLAN to which the port belongs
STATE	Type of the MAC address added. "Security" means it is a secure MAC address.
PORT INDEX	Port to which the secure MAC address belongs
AGING TIME(s)	Period of time before the secure MAC address ages out. "NOAGED" is displayed for secure MAC addresses.
x mac address(es) found	Number of secure MAC addresses stored

port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security authorization ignore** to configure a port to ignore the authorization information from the server (an RADIUS server or the local device).

Use **undo port-security authorization ignore** to restore the default.

By default, a port uses the authorization information from the server.

After a user passes RADIUS or local authentication, the server performs authorization based on the authorization attributes configured for the user's account. For example, it may assign a VLAN.

Related commands: **display port-security**.

Examples

# Configure port GigabitEthernet 1/0/1 to ignore the authorization information from the authentication server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

port-security enable

Syntax

port-security enable

undo port-security enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **port-security enable** to enable port security.

Use **undo port-security enable** to disable port security.

By default, port security is disabled.

You must disable global 802.1X and MAC authentication before you enable port security on a port.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based, and the port authorization state is auto.
- Port security mode is noRestrictions.

You cannot disable port security when online users are present.

Related commands: **display port-security**, **dot1x**, **dot1x port-method**, **dot1x port-control**, and **mac-authentication**.

Examples

# Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

port-security intrusion-mode

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. This implements illegal traffic filtering on the port. A blocked MAC address is restored to normal after being blocked for three minutes, which is fixed and cannot be changed. To view the blocked MAC address list, use the **display port-security mac-address block** command.

disableport: Disables the port permanently upon detecting an illegal frame received on the port.

disableport-temporarily: Disables the port for a specific period of time whenever it receives an illegal frame. Use **port-security timer disableport** to set the period.

Description

Use **port-security intrusion-mode** to configure the intrusion protection feature so that the port takes the pre-defined actions when intrusion protection is triggered on the port.

Use **undo port-security intrusion-mode** to restore the default.

By default, intrusion protection is disabled.

To restore the connection of the port, use the **undo shutdown** command.

Related commands: **display port-security**, **display port-security mac-address block**, and **port-security timer disableport**.

Examples

# Configure port GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection is triggered.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

port-security mac-address aging-type inactivity

Syntax

port-security mac-address aging-type inactivity

undo port-security mac-address aging-type inactivity

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security mac-address aging-type inactivity** to enable inactivity aging for secure MAC addresses (sticky or dynamic).

Use **undo port-security mac-address aging-type inactivity** to restore the default.

By default, the inactivity aging function is disabled.

If only an aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC address. When you use an aging timer together with the inactivity aging function, the aging timer restarts once traffic data is detected from the sticky MAC address The inactivity aging function prevents the unauthorized use of a secure MAC address when the authorized user is offline, and removes outdated secure MAC addresses so new secure MAC addresses can be learned.

Related commands: **port-security timer autolearn aging**, and **port-security mac-address dynamic**.

Examples

# Enable inactivity aging for secure MAC addresses on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address aging-type inactivity
```

port-security mac-address dynamic

Syntax

port-security mac-address dynamic

undo port-security mac-address dynamic

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security mac-address dynamic** to enable the dynamic secure MAC function. This function converts sticky MAC addresses to dynamic, and disables saving them to the configuration file.

Use **undo port-security mac-address dynamic** to restore the default.

By default, sticky MAC addresses can be saved to the configuration file, and once saved, survive a device reboot.

After you execute this command, you cannot manually configure sticky MAC address, and secure MAC addresses automatically learned by a port in autoLearn mode are also dynamic. All dynamic MAC addresses are lost at reboot. Use this command when you want to clear all sticky MAC addresses after a device reboot.

You can display dynamic secure MAC addresses by using the **display port-security mac-address security** command.

Related commands: **display port-security mac-address security**, **mac-address dynamic**.

Examples

# Enable the dynamic secure MAC function on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address dynamic
```

port-security mac-address security

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

undo port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

View

Layer 2 Ethernet interface view, system view

Default level

2: System level

Parameters

sticky: Specifies a sticky MAC address. If you do not provide this keyword, the command configures a static secure MAC address.

mac-address: Secure MAC address, in the H-H-H format.

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet port by its type and number.

vlan *vlan-id*: Specifies the VLAN that has the secure MAC address. The *vlan-id* argument represents the ID of the VLAN in the range of 1 to 4094. Make sure that you have assigned the Layer 2 port to the specified VLAN.

Description

Use **port-security mac-address security** to add a secure MAC address.

Use **undo port-security mac-address security** to remove a secure MAC address.

By default, no secure MAC address entry is configured.

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode. They can survive link down/up events, and once saved, can survive a device reboot. You can bind a MAC address to only one port in a VLAN.

When a port is operating in autoLearn mode, you can add important or frequently used MAC addresses as sticky or static secure MAC addresses to avoid the secure MAC address limit causing authentication failure.

Static secure MAC addresses never age out unless you remove them by using the **undo port-security mac-address security** command, changing the port security mode, or disabling the port security feature.

Sticky MAC addresses can be manually configured or automatically learned in autoLearn mode. Sticky MAC addresses do not age out by default. You can use the **port-security timer autolearn aging** command to set an aging timer for them. When the timer expires, the sticky MAC addresses are removed.

You cannot change the type of a secure address entry that has been added or add two entries that are identical except for their entry type. For example, you cannot add the **port-security mac-address security sticky 1-1-1 vlan 10** entry when a **port-security mac-address security 1-1-1 vlan 10** entry exists. To add the new entry, you must delete the old entry.

To enable port security on a port, use the **port-security enable** command, and to set the port in autoLearn mode, use the **port-security port-mode autolearn** command.

Related commands: **display port-security** and **port-security timer autolearn aging**.

Examples

# Enable port security, set port GigabitEthernet 1/0/1 in autoLearn mode, and add a static secure MAC address 0001-0001-0002 in VLAN 10.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet
1/0/1 vlan 10
```

# Enable port security, set port GigabitEthernet 1/0/1 in autoLearn mode, and add a static secure MAC address 0001-0002-0003 in VLAN 4 in interface view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] port-security mac-address security 0001-0002-0003 vlan 4
```

port-security max-mac-count

Syntax

port-security max-mac-count *count-value*

undo port-security max-mac-count

View

Ethernet interface view

Default level

2: System level

Parameters

count-value: Specifies the maximum number of MAC addresses that port security allows on the port. The value is in the range of 1 to 1024.

Description

Use **port-security max-mac-count** to set the maximum number of MAC addresses that port security allows on a port.

Use **undo port-security max-mac-count** to restore the default setting.

By default, port security has no limit on the number of MAC addresses on a port.

In autoLearn mode, this command sets the maximum number of secure MAC addresses (both configured and automatically learned) on the port.

In any other mode that enables 802.1X, MAC authentication, or both, this command sets the maximum number of authenticated MAC addresses on the port. The actual maximum number of concurrent users that the port accepts equals this limit or the authentication method's limit on the number of concurrent users, whichever is smaller. For example, in userLoginSecureExt mode, if 802.1X allows less concurrent users than port security's limit on the number of MAC addresses, port security's limit takes effect.

You cannot change port security's limit on the number of MAC addresses when the port is operating in **autoLearn** mode.

Related commands: **display port-security**.

Examples

# Set port security's limit on the number of MAC addresses to 100 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

port-security ntk-mode

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

View

Ethernet interface view

Default level

2: System level

Parameters

ntk-withbroadcasts: Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.

ntk-withmulticasts: Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

ntkonly: Forwards only unicast frames with authenticated destination MAC addresses.

Description

Use **port-security ntk-mode** to configure the NTK feature.

Use **undo port-security ntk-mode** to restore the default.

By default, NTK is disabled on a port and all frames are allowed to be sent.

The need to know (NTK) feature checks the destination MAC addresses in outbound frames to allow frames to be sent to only devices passing authentication, preventing illegal devices from intercepting network traffic.

Related commands: **display port-security**.

Examples

# Set the NTK mode of port GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets to only devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

port-security oui

Syntax

port-security oui *oui-value* **index** *index-value*

undo port-security oui index *index-value*

View

System view

Default level

2: System level

Parameters

oui-value: Specifies an organizationally unique identifier (OUI) string, a 48-bit MAC address in the H-H-H format. The system uses only the 24 high-order bits as the OUI value.

index-value: Specifies the OUI index, in the range of 1 to 16.

Description

Use **port-security oui** to configure an OUI value for user authentication. This value is used when the port security mode is userLoginWithOUI.

Use **undo port-security oui** to delete the OUI value with the specified OUI index.

By default, no OUI value is configured.

An OUI, the first 24 binary bits of a MAC address, is assigned by IEEE to uniquely identify a device vendor. Use this command when you configure a device to allow packets from certain wired devices to pass authentication or to allow packets from certain wireless devices to initiate authentication. For example, when a company allows only IP phones of vendor A in the Intranet, use this command to set the OUI of vendor A.

Related commands: **display port-security**.

Examples

# Configure an OUI value of 000d2a, setting the index to 4.

```
<Sysname> system-view
[Sysname] port-security oui 000d-2a10-0033 index 4
```

port-security port-mode

Syntax

port-security port-mode { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }

undo port-security port-mode

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

Keyword	Security mode	Description
autolearn	autoLearn	In this mode, a port can learn MAC addresses, and allows frames sourced from learned or configured the MAC addresses to pass. The dynamically learned MAC addresses are secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command. A secure MAC address never ages out by default. In addition, you can configure MAC addresses manually by using the **mac-address dynamic** and **mac-address static** commands for a port in autoLearn mode. When the number of secure MAC addresses reaches the upper limit set by the **port-security max-mac-count** command, the port changes to secure mode.
mac-authentication	macAddressWithRadius	In this mode, a port performs MAC authentication for users and services multiple users.
mac-else-userlogin-secure	macAddressElseUserLoginSecure	This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority. • A port performs MAC authentication 30 seconds after receiving non-802.1X frames. • Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	Similar to the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.
secure	secure	In this mode, MAC address learning is disabled on the port and you can configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. The port permits only frames sourced from secure MAC addresses and MAC addresses you manually configured by using the **mac-address static** and **mac-address dynamic** commands.

Keyword	Security mode	Description
userlogin	userLogin	In this mode, a port performs 802.1X authentication and implements port-based access control. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication.
userlogin-secure	userLoginSecure	In this mode, a port performs 802.1X authentication and implements MAC-based access control. It services only one user passing 802.1X authentication.
userlogin-secure-ext	userLoginSecureExt	Similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.
userlogin-secure-or-mac	macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes. For wired users, the port performs MAC authentication 30 seconds after receiving non-802.1X frames and performs 802.1X authentication upon receiving 802.1X frames.
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	Similar to the macAddressOrUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.
userlogin-withoui	userLoginWithOUI	Similar to the userLoginSecure mode. In addition, a port in this mode also permits frames from a user whose MAC address contains a specific OUI (organizationally unique identifier). For wired users, the port performs 802.1X authentication upon receiving 802.1X frames, and performs OUI check upon receiving non-802.1X frames.

Description

Use **port-security port-mode** to set the port security mode of a port.

Use **undo port-security port-mode** to restore the default.

By default, a port operates in noRestrictions mode, where port security does not take effect.

To change the security mode of a port security enabled port, you must set the port in noRestictions mode first. When the port has online users, you cannot change port security mode.

IMPORTANT:

If you are configuring the autoLearn mode, first set port security's limit on the number of MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

When port security is enabled, you cannot manually enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

Related commands: **display port-security**.

Examples

# Enable port security and set port GigabitEthernet 1/0/1 in secure mode.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
```

# Change the port security mode of port GigabitEthernet 1/0/1 to userLogin.

```
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

port-security timer autolearn aging

Syntax

port-security timer autolearn aging *time-value*

undo port-security timer autolearn aging

View

System view

Default level

2: System level

Parameters

time-value: Sets the aging timer in minutes for secure MAC addresses. The value is in the range of 0 to 129600. To disable the aging timer, set the timer to 0.

Description

Use **port-security timer autolearn aging** to set the secure MAC aging timer. The timer applies to all sticky or dynamic secure MAC addresses.

Use **undo port-security timer autolearn aging** to restore the default.

By default, secure MAC addresses never age out.

Related commands: **display port-security** and **port-security mac-address security**.

Examples

# Set the secure MAC aging timer to 30 minutes.

```
<Sysname> system-view
[Sysname] port-security timer autolearn aging 30
```

port-security timer disableport

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

View

System view

Default level

2: System level

Parameters

time-value: Specifies the silence period during which the port remains disabled, in seconds. It is in the range of 20 to 300.

Description

Use **port-security timer disableport** to set the silence period during which the port remains disabled.

Use **undo port-security timer disableport** to restore the default.

By default, the silence period is 20 seconds.

If you configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame, use this command to set the silence period.

Related commands: **display port-security**.

Examples

# Configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame and set the silence period to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

port-security trap

Syntax

port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

undo port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

View

System view

Default level

2: System level

Parameters

addresslearned: Enables MAC address learning traps. The port security module sends traps when a port learns a new MAC address.

dot1xlogfailure: Enables 802.1X authentication failure traps. The port security module sends traps when an 802.1X authentication fails.

dot1xlogon: Enables 802.1X authentication success traps. The port security module sends traps when an 802.1X authentication is passed.

dot1xlogoff: Enables 802.1X user logoff event traps. The port security module sends traps when an 802.1X user is logged off.

intrusion: Enables intrusion traps. The port security module sends traps when it detects illegal frames.

ralmlogfailure: Enables MAC authentication failure traps. The port security module sends traps when a MAC authentication fails.

ralmlogoff: Enables MAC authentication user logoff traps. The port security module sends traps when a MAC authentication user is logged off.

ralmlogon: Enables MAC authentication success traps. The port security module sends traps when a MAC authentication is passed.

NOTE:

RALM (RADIUS Authenticated Login using MAC-address) means RADIUS authentication based on MAC address.

Description

Use **port-security trap** to enable port security traps.

Use **undo port-security trap** to disable port security traps.

By default, port security traps are disabled.

You can enable certain port security traps for monitoring user behaviors.

Related commands: **display port-security**.

Examples

# Enable MAC address learning traps.

```
<Sysname> system-view
[Sysname] port-security trap addresslearned
```

User profile configuration commands

display user-profile

Syntax

display user-profile [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display user-profile** to display information about all user profiles that have been created.

Examples

# Display information about all user profiles that have been created.

```
<Sysname> display user-profile
Status    User profile
enabled   a123
        ----Total user profiles:        1-------
        ----Enabled user profiles:      1-------
```

Table 20 Command output

Field	Description
Status	Status of the user profile: • enabled • disabled
User profile	User profile name
Total user profiles	Total number of user profiles that have been created
Enabled user profiles	Total number of user profiles that have been enabled

user-profile enable

Syntax

user-profile *profile-name* **enable**

undo user-profile *profile-name* **enable**

View

System view

Default level

2: System level

Parameters

profile-name: Specifies a user profile name, a case-sensitive string of 1 to 31 characters. It can only contain English letters, digits, and underlines, and it must start with an English letter. The user profile must already exist.

Description

Use **user-profile enable** to enable a user profile that has been created. If the user profile does not exist, the command fails. Only enabled user profiles can be applied to authenticated users.

Use **undo user-profile enable** to disable the specified user profile. Disabling a user profile logs out users that are using the user profile. To edit or remove the configurations in a user profile, disable the user profile first.

By default, a created user profile is disabled.

Examples

# Enable user profile **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123 enable
```

user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

Default level

2: System level

Parameters

profile-name: Assigns a name to the user profile. The name is a case-sensitive string of 1 to 31 characters. It can only contain English letters, digits, and underlines, and it must start with an English letter. A user profile name must be globally unique.

Description

Use **user-profile** to create a user profile and enter the user profile view. If the specified user profile has been created, you enter the user profile view directly.

Use **undo user-profile** to remove an existing disabled user profile. You cannot remove a user profile that is enabled.

By default, no user profiles exist on the device.

Related commands: **user-profile enable**.

Examples

# Create user profile **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

# Enter the user profile view of **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

Password control configuration commands

display password-control

Syntax

display password-control [**super**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

super: Displays the password control information of the super passwords. Without this keyword, the command displays the password control information for all passwords.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display password-control** to display password control configuration information.

Examples

# Display the global password control configuration information.

```
<Sysname> display password-control
Global password control configurations:
 Password control:                     Disabled
 Password aging:                       Enabled (90 days)
 Password length:                      Enabled (10 characters)
 Password composition:                 Enabled (1 types,  1 characters per type)
 Password history:                     Enabled (max history records:4)
 Early notice on password expiration: 7 days
 User authentication timeout:          60 seconds
 Maximum failed login attempts:        3 times
 Login attempt-failed action:          Lock for 1 minutes
 Minimum password update time:         24 hours
 User account idle-time:               90 days
 Login with aged password:             3 times in 30 days
 Password complexity:                  Disabled (username checking)
                                       Disabled (repeated characters checking)
```

# Display the password control configuration information for super passwords.

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                      Enabled (90 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (1 types,  1 characters per type)
```

Table 21 Command output

Field	Description
Password control	Whether the password control feature is enabled
Password aging	Whether password aging is enabled and, if enabled, the aging time
Password length	Whether the minimum password length restriction function is enabled and, if enabled, the setting
Password composition	Whether the password composition restriction function is enabled and, if enabled, the settings
Password history	Whether the password history function is enabled and, if enabled, the setting
Early notice on password expiration	Number of days during which the user is warned of the pending password expiration
User authentication timeout	Password authentication timeout time
Maximum failed login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users
Login attempt-failed action	Action to be taken after a user fails to login for the specified number of attempts
Minimum password update time	Minimum password update interval
User account idle-time	Maximum account idle time
Login with aged password	Number of times and maximum number of days a user can log in using an expired password
Password complexity	Whether to check the password complexity, including: • Checking whether a password contains the username or the reverse of the username • Checking whether a password contains any character that is repeated consecutively three or more times

display password-control blacklist

Syntax

display password-control blacklist [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

user-name *name*: Specifies a user by the name, a string of 1 to 80 characters.

ip *ipv4-address*: Specifies the IPv4 address of a user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display password-control blacklist** to display information about users blacklisted due to authentication failure.

With no arguments provided, this command displays information about all users in the blacklist.

Examples

# Display information about users blacklisted due to authentication failure.

```
<Sysname> display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 1      Lock flag: unlock

Total 1 blacklist item(s) matched. 1 listed.
```

Table 22 Command output

Field	Description
Username	Username of the user
IP	IP address of the user
Login failed times	Number of login failures
Lock flag	Whether the user is prohibited from logging in: • **unlock**—Not prohibited • **lock**—Prohibited temporarily or permanently, depending on the **password-control login-attempt** command

password

Syntax

Password

undo password

View

Local user view

Default level

2: System level

Parameters

None

Description

Use **password** to set a password for a local user in interactive mode.

Use **undo password** to remove the password for a local user.

Valid characters for a local user password include uppercase letters A to Z, lowercase letters a to z, numbers 0 to 9, blank space, and these 31 symbols: ~`!@#$%^&*()_+-={}|[]\:";'<>,./.

A local user password configured in interactive mode must satisfy the password control requirement. For example, if the minimum password length is set to 8, the password must contain at least eight characters.

Examples

# Set a password for local user **test** in interactive mode.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password
Password:**********
Confirm :**********
Updating user(s) information, please wait....
```

password-control { aging | composition | history | length } enable

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

View

System view

Default level

2: System level

Parameters

aging: Enables the password aging function.

composition: Enables the password composition restriction function.

history: Enables the password history function.

length: Enables the minimum password length restriction function.

Description

Use **password-control** { **aging** | **composition** | **history** | **length** } **enable** to enable the password aging, composition restriction, history, or minimum password length restriction function.

Use **undo password-control** { **aging** | **composition** | **history** | **length** } **enable** to disable the specified function.

By default, the four password control functions are all enabled.

For these four functions to take effect, the password control feature must be enabled globally.

You must enable a function for its relevant configurations to take effect. For example, if the minimum password length restriction function is not enabled, the setting by the **password-control length** command does not take effect.

The system stops recording history passwords after you execute the **undo password-control history enable** command, but the prior records still exist.

Related commands: **password-control enable** and **display password-control**.

Examples

# Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

# Enable the password composition restriction function.

```
[Sysname] password-control composition enable
```

# Enable the password aging function.

```
[Sysname] password-control aging  enable
```

# Enable the minimum password length restriction function.

```
[Sysname] password-control length  enable
```

# Enable the password history function.

```
[Sysname] password-control history  enable
```

password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

View

System view, user group view, local user view

Default level

2: System level

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Description

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

By default, the global password aging time is 90 days, the password aging time of a user group equals the global setting, and the password aging time of a local user equals that of the user group to which the local user belongs.

The setting in system view has global significance and applies to all user groups, the setting in user group view applies to all local users in the user group, and the setting in local user view applies to only the local user.

A password aging time setting with a smaller application range has a higher priority. That is, the system prefers the setting for a local user. If there is no setting for the local user, the system will use the setting for the user group. If there is no setting for the user group, the system will use the global setting.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

# Set the global password aging time to 80 days.

```
<Sysname> system-view
[Sysname] password-control aging 80
```

# Set the password aging time for user group **test** to 90 days.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control aging 90
[Sysname-ugroup-test] quit
```

# Set the password aging time for local user **abc** to 100 days.

```
[Sysname] local-user abc
[Sysname-luser-abc] password-control aging 100
```

password-control alert-before-expire

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

View

System view

Default level

2: System level

Parameters

alert-time: Specifies the number of days before a user's password expires during which the user is warned of the pending password expiration, in the range of 1 to 30.

Description

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is warned of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

By default, a user is warned of pending password expiration 7 days before the user's password expires.

Examples

# Configure the device to warn a user about pending password expiration 10 days before the user's password expires.

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

password-control authentication-timeout

Syntax

password-control authentication-timeout *authentication-timeout*

undo password-control authentication-timeout

View

System view

Default level

2: System level

Parameters

authentication-timeout: Specifies the user authentication timeout time in seconds, in the range of 30 to 120.

Description

Use **password-control authentication-timeout** to set the user authentication timeout time.

Use **undo password-control authentication-timeout** to restore the default.

By default, the user authentication timeout time is 60 seconds.

Examples

# Set the user authentication timeout time to 40 seconds.

```
<Sysname> system-view
[Sysname] password-control authentication-timeout 40
```

password-control complexity

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

View

System view

Default level

2: System level

Parameters

same-character: Refuses a password that contains any character repeated consecutively three or more times.

user-name: Refuses a password that contains the username or the reverse of the username.

Description

Use **password-control complexity** to configure the password complexity checking policy. Unqualified passwords will be refused.

Use **undo password-control complexity check** to remove a password complexity checking item.

By default, no user password complexity checking is performed, and a password can contain the username, the reverse of the username, or a character repeated three or more times consecutively.

Related commands: **display password-control**.

Examples

# Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Sysname> system-view
[Sysname] password-control complexity user-name check
```

password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

View

System view, user group view, local user view

Default level

2: System level

Parameters

type-number *type-number*: Specifies the minimum number of password composition types, in the range of 1 to 4.

type-length *type-length*: Specifies the minimum number of characters of each password composition type, in the range of 1 to 63.

Description

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

By default, the global password composition policy is as follows: the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is also 1. The default password composition policy of a user group is the same as the global policy, and the default password composition policy of a local user is the same as that of the user group to which the local user belongs.

The settings in system view have global significance and apply to all user groups, the settings in user group view apply to all local users in the user group, and the settings in local user view apply to only the local user.

A password composition policy with a smaller application range has a higher priority. That is, the system prefers the settings for a local user. If there is no setting for the local user, the system will use the settings for the user group. If there is no setting for the user group, the system will use the global settings.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

# Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for all passwords.

```
<Sysname> system-view
[Sysname] password-control composition type-number 3 type-length 5
```

# Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for user group **test**.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 3 type-length 5
[Sysname-ugroup-test] quit
```

# Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for local user **abc**.

```
[Sysname] local-user abc
[Sysname-luser-abc] password-control composition type-number 3 type-length 5
```

password-control enable

Syntax

password-control enable

undo password-control enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **password-control enable** to enable the password control feature globally.

Use **undo password-control enable** to disable the password control feature globally.

By default, the password control feature is disabled globally.

Only after the password control feature is enabled globally, do the password control functions take effect.

Related commands: **display password-control**.

Examples

# Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

password-control expired-user-login

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

View

System view

Default level

2: System level

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. It must be in the range of 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires, in the range of 0 to 10. 0 means that a user cannot log in after the password expires.

Description

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

By default, a user can log in three times within 30 days after the password expires.

Related commands: **display password-control**.

Examples

# Specify that a user can log in five times within 60 days after the password expires.

```
<Sysname> system-view
[Sysname] password-control expired-user-login delay 60 times 5
```

password-control history

Syntax

password-control history *max-record-num*

undo password-control history

View

System view

Default level

2: System level

Parameters

max-record-num: Specifies the maximum number of history password records for each user, in the range of 2 to 15.

Description

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

By default, the maximum number of history password records for each user is 4.

Examples

# Set the maximum number of history password records for each user to 10.

```
<Sysname> system-view
[Sysname] password-control history 10
```

password-control length

Syntax

password-control length *length*

undo password-control length

View

System view, user group view, local user view

Default level

2: System level

Parameters

length: Specifies the minimum password length in characters, in the range of 4 to 32.

Description

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

By default, the global minimum password length is 10 characters, the minimum password length of a user group equals the global setting, and the minimum password length of a local user equals that of the user group to which the local user belongs.

The setting in system view has global significance and applies to all user groups, the setting in user group view applies to all local users in the user group, and the setting in local user view applies to only the local user.

A minimum password length setting with a smaller application range has a higher priority. That is, the system prefers the setting for a local user. If there is no setting for the local user, the system will use the setting for the user group. If there is no setting for the user group, the system will use the global setting.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

# Set the global minimum password length to 9 characters.

```
<Sysname> system-view
[Sysname] password-control length 9
```

# Set the minimum password length to 9 characters for user group **test**.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 9
[Sysname-ugroup-test] quit
```

# Set the minimum password length to 9 characters for local user **abc**.

```
[Sysname] local-user abc
[Sysname-luser-abc] password-control length 9
```

password-control login idle-time

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

View

System view

Default level

2: System level

Parameters

idle-time: Specifies the maximum account idle time, in the range of 0 to 365, in days. 0 means no restriction for account idle time.

Description

Use **password-control login idle-time** to set the maximum account idle time. If a user account is idle for this period of time, it becomes invalid.

Use **undo password-control login idle-time** to restore the default.

By default, the maximum account idle time is 90 days.

Related commands: **display password-control**.

Examples

# Set the maximum account idle time to 30 days.

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

password-control login-attempt

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

View

System view

Default level

2: System level

Parameters

login-times: Specifies the maximum number of consecutive failed login attempts, in the range of 2 to 10.

exceed: Specifies the action to be taken when a user fails to log in after the specified number of attempts.

lock: Permanently prohibits a user who fails to log in after the specified number of attempts from logging in.

lock-time *time*: Forces a user who fails to log in after the specified number of attempts to wait for a period of time before trying again. The *time* argument is in minutes and in the range of 1 to 360.

unlock: Allows a user who fails to log in after the specified number of attempts to continue trying to log in.

Description

Use **password-control login-attempt** to specify the maximum number of consecutive failed login attempts and the action to be taken when a user fails to log in after the specified number of attempts.

Use **undo password-control** to restore the default.

By default, the maximum number of consecutive failed login attempts is three and a user failing to log in after the specified number of attempts must wait for one minute before trying again.

If prohibited permanently, a user can log in only after you remove the user from the blacklist.

If prohibited temporarily, a user can log in again after the lock time elapses or an administrator removes the user from the blacklist.

If not prohibited to log in, a user is removed from the blacklist as long as the user logs in successfully or after the blacklist aging time (one minute) elapses.

Related commands: **display password-control**, **display password-control blacklist**, and **reset password-control blacklist**.

Examples

# Set the maximum number of login attempts to four and permanently prohibit a user failing to log in after four attempts from logging in.

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

Later, if a user tries to log in but fails four times, you can find it in the blacklist, with its status changed from **unlock** to **lock**:

```
[Sysname] display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 4      Lock flag: lock

Total 1 blacklist item(s) matched.
```

The user can no longer log in.

# Set the maximum number of login attempts to two and prohibit a user failing to log in after two attempts from logging in within three minutes.

```
<Sysname> system-view
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

Later, if a user tries to log in but fails two times, you can find it in the blacklist, with its status changed from unlock to lock:

```
[Sysname] display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 2      Lock flag: lock

Total 1 blacklist item(s) matched.
```

After three minutes, the user is removed from the blacklist and can log in again.

password-control password update interval

Syntax

password-control password update interval *interval*

undo password-control password update interval

View

System view

Default level

2: System level

Parameters

interval: Specifies the minimum password update interval, in the range of 0 to 168, in hours. 0 means no requirements for password update interval.

Description

Use **password-control password update interval** to set the minimum password update interval, that is, the minimum interval at which users can change their passwords.

Use **undo password-control password update interval** to restore the default.

By default, the minimum password update interval is 24 hours.

This function is not effective in the case that a user is prompted to change the password when the user logs in for the first time or after the password is aged out.

Related commands: **display password-control**.

Examples

# Set the minimum password update interval to 36 hours.

```
<Sysname> system-view
[Sysname] password-control password update interval 36
```

password-control super aging

Syntax

password-control super aging *aging-time*

undo password-control super aging

View

System view

Default level

2: System level

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Description

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

By default, the aging time for super passwords is 90 days.

The setting for super passwords, if present, overrides that for all passwords.

Related commands: **password-control aging**.

Examples

# Set the aging time for super passwords to 10 days.

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

View

System view

Default level

2: System level

Parameters

type-number *type-number*: Specifies the minimum number of composition types for super passwords, in the range of 1 to 4.

type-length *type-length*: Specifies the minimum number of characters of each composition type for super passwords, in the range of 1 to 16.

Description

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

By default, both the minimum number of composition types and the minimum number of characters of composition type are 1 for super passwords.

The settings for super passwords, if present, override those configured for all passwords.

Related commands: **password-control composition**.

Examples

# Set the minimum number of composition types to 3 and the minimum number of characters of each composition type to 5 for super passwords.

```
<Sysname> system-view
[Sysname] password-control super composition type-number 3  type-length 5
```

password-control super length

Syntax

password-control super length *length*

undo password-control super length

View

System view

Default level

2: System level

Parameters

length: Specifies the minimum length for super passwords in characters, in the range of 4 to 16.

Description

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

By default, the minimum super password length is 10 characters.

The setting for super passwords, if present, overrides that for all passwords.

Related commands: **password-control length**.

Examples

# Set the minimum length for super passwords to 10 characters.

```
<Sysname> system-view
[Sysname] password-control super length 10
```

reset password-control blacklist

Syntax

reset password-control blacklist [**user-name** *name*]

View

User view

Default level

3: Manage level

Parameters

user-name *name*: Specifies the username of the user to be removed from the blacklist. *name* is a case-sensitive string of 1 to 80 characters.

Description

Use **reset password-control blacklist** to remove all or one user from the blacklist.

Related commands: **display password-control blacklist**.

Examples

# Delete the user named **test** from the blacklist.

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

reset password-control history-record

Syntax

reset password-control history-record [**user-name** *name* | **super** [**level** *level*]]

View

User view

Default level

3: Manage level

Parameters

user-name *name*: Specifies the username of the user whose password records are to be deleted. *name* is a case-sensitive string of 1 to 80 characters.

super: Deletes the history records of the super password specified by the **level** *level* combination or the history records of all super passwords.

level *level*: Specifies a user level, in the range of 1 to 3.

Description

Use **reset password-control history-record** to delete history password records.

With no arguments or keywords specified, this command deletes the history password records of all local users.

With the **super** keyword specified but the *level* argument not specified, this command deletes the history records of all super passwords.

Examples

# Clear the history password records of all local users (enter Y to confirm).

```
<Sysname> reset password-control history-record
   Are you sure to delete all local user's history records? [Y/N]:
```

HABP configuration commands

display habp

Syntax

display habp [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp** to display HABP configuration information.

If the HABP function is not enabled on the device, this command does not display the HABP configuration but only the running status of the HABP function.

Examples

# Display HABP configuration information.

```
<Sysname> display habp
Global HABP information:
    HABP Mode: Server
    Sending HABP request packets every 20 seconds
    Bypass VLAN: 2
```

Table 23 Command output

Field	Description
HABP Mode	HABP mode of the current device, server or client.
Sending HABP request packets every 20 seconds	The HABP server sends HABP request packets at an interval of 20 seconds.
Bypass VLAN	ID of the VLAN in which HABP packets are transmitted.

display habp table

Syntax

display habp table [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp table** to display HABP MAC address table entries.

This command is applicable only on an HABP server to display the MAC address entries collected by the HABP server.

Examples

# On the HABP server, display HABP MAC address table entries.

```
<Sysname> display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        GigabitEthernet1/0/1
```

Table 24 Command output

Field	Description
MAC	MAC address.
Holdtime	Lifetime of an entry in seconds. The initial value is three times the interval to send HABP request packets. An entry will age out if it is not updated during the period.
Receive Port	Port that learned the MAC address.

display habp traffic

Syntax

display habp traffic [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp traffic** to display HABP packet statistics.

Examples

# Display HABP packet statistics.

```
<Sysname> display habp traffic
HABP counters :
         Packets output: 48, Input: 36
         ID error: 0, Type error: 0, Version error: 0
         Sent failed: 0
```

Table 25 Command output

Field	Description
Packets output	Number of HABP packets sent
Input	Number of HABP packets received
ID error	Number of packets with an incorrect ID
Type error	Number of packets with an incorrect type
Version error	Number of packets with an incorrect version number
Sent failed	Number of packets that failed to be sent

habp client vlan

Syntax

habp client vlan *vlan-id*

undo habp client

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies the ID of the VLAN in which HABP packets are to be transmitted, in the range of 1 to 4094.

Description

Use **habp client vlan** to specify the VLAN to which the HABP client belongs. HABP packets are to be transmitted in this VLAN.

Use **undo habp client** to restore the default.

By default, an HABP client belongs to VLAN 1.

Examples

# Specify the HABP client to belong to VLAN 2.

```
<Sysname> system-view
[Sysname] habp client vlan 2
```

habp enable

Syntax

habp enable

undo habp enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **habp enable** to enable HABP.

Use **undo habp enable** to disable HABP.

By default, HABP is enabled.

Examples

# Enable HABP.

```
<Sysname> system-view
[Sysname] habp enable
```

habp server vlan

Syntax

habp server vlan *vlan-id*

undo habp server

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies the ID of the VLAN in which HABP packets are to be transmitted, in the range of 1 to 4094.

Description

Use **habp server vlan** to configure HABP to operate in server mode and specify the VLAN in which HABP packets are to be transmitted.

Use **undo habp server** to configure HABP to operate in the default mode.

By default, HABP operates in client mode.

In a cluster, if a member switch with 802.1X authentication or MAC authentication enabled is attached with some other member switches of the cluster, you also need to configure HABP server on this device. Otherwise, the cluster management device will not be able to manage the devices attached to this member switch. For information about the cluster function, see *Network Management and Monitoring Configuration Guide*.

Examples

# Configure HABP to operate in server mode and specify the VLAN for HABP packets as VLAN 2.

```
<Sysname> system-view
[Sysname] habp server vlan 2
```

habp timer

Syntax

habp timer *interval*

undo habp timer

View

System view

Default level

2: System level

Parameters

interval: Specifies the interval (in seconds) at which the switch sends HABP request packets, in the range of 5 to 600.

Description

Use **habp timer** to set the interval at which the switch sends HABP request packets.

Use **undo habp timer** to restore the default.

The default interval is 20 seconds.

This command is required only on the HABP server.

Examples

# Set the interval at which the switch sends HABP request packets to 50 seconds.

```
<Sysname> system-view
[Sysname] habp timer 50
```

Public key configuration commands

display public-key local public

Syntax

display public-key local { **dsa** | **rsa** } **public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dsa: Specifies a DSA key pair.

rsa: Specifies an RSA key pair.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display public-key local public** to display the public key information of the local asymmetric key pairs.

Related commands: **public-key local create**.

Examples

# Display the public key information of the local RSA key pairs.

```
<Sysname> display public-key local rsa public

=====================================================
Time of Key pair created: 19:59:16  2012/03/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A633BA0F1DB01F
84EB51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D049143656F1287502C06D39D39F
28F0F5CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCDB5DB620CD1F471401B711713970234844
4A2D8900497A87B8D5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF30203010001

=====================================================
Time of Key pair created: 19:59:17  2012/03/07
```

```
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2AACC7B2AE12
B2B1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27E054BFAA0A85E113FBDE75
1EE0ECEF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

# Display the public key information of the local DSA key pair.

```
<Sysname> display public-key local dsa public

=====================================================
Time of Key pair created: 20:00:16  2012/03/07
Key name: HOST_KEY
Key type: DSA Encryption Key
=====================================================
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F
0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26
CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F067
8D7722B5341C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30
F48EDACE915F0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF931
33E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC
717B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585
DA7F42519718CC9B09EEF0381850002818100CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB
374D677A7A6124EBABD59FE48796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F72E80DBE337CB29989
A23378EB21C38EE083F11ED6DC8D4DBE001BA85450CEA071C2A471C83761E4CF32C174B418612CDD597B4
41F0CAA05DC01CB93A0ABB247C06FBA4C79054
```

Table 26 Command output

Field	Description
Time of Key pair created	Date and time when the local asymmetric key pair was created.
Key name	Key name: • **HOST_KEY**—Host public key. • **SERVER_KEY**—Server public key. This value is available only for RSA key pairs.
Key type	Key type: • **RSA Encryption Key**—RSA key pair. • **DSA Encryption Key**—DSA key pair.
Key code	Public key data

display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays brief information about all peer public keys.

name *publickey-name*: Displays information about a peer public key. *publickey-name* represents a public key by its name, a case-sensitive string of 1 to 64 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display public-key peer** to display information about the specified or all peer public keys on the local device.

With neither the **brief** keyword nor the **name** *publickey-name* option specified, the command displays detailed information about all locally saved peer public keys.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to get a local copy of a peer public key.

Related commands: **public-key peer** and **public-key peer import sshkey**.

Examples

# Display detailed information about the peer host public key named **idrsa**.

```
<Sysname> display public-key peer name idrsa
=====================================
  Key Name  : idrsa
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B003081870281810 09C46A8710216CEC0C01C7CE136B
A76C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB74
42D56393BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846
B7CB9A7757C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

Table 27 Command output

Field	Description
Key Name	Name of the public key
Key Type	Key type, which can be RSA or DSA.
Key Module	Key modulus length in bits
Key Code	Public key data

# Display brief information about all locally saved peer public keys.

```
<Sysname> display public-key peer brief
Type  Module  Name
---------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 28 Command output

Field	Description
Type	Key type, RSA or DSA.
Module	Key modulus length in bits
Name	Name of the public key

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Default level

2: System level

Parameters

None

Description

Use **peer-public-key end** to return from public key view to system view.

Related commands: **public-key peer**.

Examples

# Exit public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
[Sysname]
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Default level

2: System level

Parameters

None

Description

Use **public-key-code begin** to enter public key code view. Then input the key data in the correct format to specify the peer public key. Spaces and carriage returns are allowed between characters.

If the peer device is an HP device, input the key data displayed by the **display public-key local public** command so that the key is format compliant.

Related commands: **public-key peer** and **public-key-code end**.

Examples

# Enter public key code view and input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC
8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164
3135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6
B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1
DDE675AC30CB020301
[Sysname-pkey-key-code]0001
```

public-key-code end

Syntax

public-key-code end

View

Public key code view

Default level

2: System level

Parameters

None

Description

Use **public-key-code end** to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, the system saves the key.

Related commands: **public-key peer** and **public-key-code begin**.

Examples

# Exit public key code view and save the configured public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
```

```
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC
8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164
3135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6
B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1
DDE675AC30CB020301
[Sysname-pkey-key-code]0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

public-key local create

Syntax

public-key local create { **dsa** | **rsa** }

View

System view

Default level

2: System level

Parameters

dsa: Specifies a DSA key pair.

rsa: Specifies an RSA key pair.

Description

Use **public-key local create** to create local asymmetric key pairs. The created local key pairs are saved automatically, and can survive a reboot.

By default, no asymmetric key pair is created.

When using this command to create DSA or RSA key pairs, you are asked to provide the length of the key modulus. The modulus length is in the range of 512 to 2048 bits, and defaults to 1024 bits. If the type of key pair already exists, the system asks you whether you want to overwrite it.

Related commands: **public-key local destroy** and **display public-key local public**.

Examples

# Create local RSA key pairs.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++
+++++++
+++++++++
+++
```

# Create a local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++.++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

public-key local destroy

Syntax

public-key local destroy { **dsa** | **rsa** }

View

System view

Default level

2: System level

Parameters

dsa: DSA key pair.

rsa: RSA key pair.

Description

Use **public-key local destroy** to destroy the local asymmetric key pairs.

Related commands: **public-key local create**.

Examples

# Destroy the local RSA key pairs.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
```

# Destroy the local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] :y
```

public-key local export dsa

Syntax

public-key local export dsa { **openssh** | **ssh2** } [*filename*]

View

System view

Default level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.0.

filename: Specifies the name of the file for storing the local public key. For more information about file name, see *Fundamentals Configuration Guide*.

Description

Use **public-key local export dsa** without the *filename* argument to display the host public key of the local DSA key pair in the specified format.

Use **public-key local export dsa** with the *filename* argument to export the host public key of the local DSA key pair to the specified file.

SSH2.0 and OpenSSH are two different public key formats for different requirements.

Related commands: **public-key local create** and **public-key local destroy**.

Examples

# Export the local DSA host public key in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

# Display the local DSA host public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20120307"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatp
RjxsSrhXFVIdRjxw59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOL
o2/RyGqDJIqB4FQwmrkwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22
---- END SSH2 PUBLIC KEY ----
```

# Display the local DSA host public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
```

```
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatp
RjxsSrhXFVIdRjxw59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOL
o2/RyGqDJIqB4FQwmrkwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22 dsa-key
```

public-key local export rsa

Syntax

public-key local export rsa { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

Default level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh1: Uses the format of SSH1.5.

ssh2: Uses the format of SSH2.0.

filename: Specifies the name of the file for storing the host public key. For more information about file name, see *Fundamentals Configuration Guide*.

Description

Use **public-key local export rsa** without the *filename* argument to display the host public key of the local RSA key pairs in the specified key format.

Use **public-key local export rsa** with the *filename* argument to export the host public key of the local RSA key pairs to the specified file.

SSH1, SSH2.0 and OpenSSH are three different public key formats for different requirements.

Related commands: **public-key local create** and **public-key local destroy**.

Examples

# Export the host public key of the local RSA key pairs in OpenSSH format to the file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

# Display the host public key of the local RSA key pairs in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20120307"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6u
t5NIc5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j
+o0MpOpzh3W768/+u1riz+1LcwVTs51Q==
---- END SSH2 PUBLIC KEY ----
```

# Display the host public key of the local RSA key pairs in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6u
t5NIc5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j
+o0MpOpzh3W768/+u1riz+1LcwVTs51Q== rsa-key
```

public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

View

System view

Default level

2: System level

Parameters

keyname: Specifies a name for the peer public key on the local device, a case-sensitive string of 1 to 64 characters.

Description

Use **public-key peer** to specify a name for the peer public key and enter public key view.

Use **undo public-key peer** to remove the public key.

To manually configure the peer public key on the local device, obtain the public key in hexadecimal from the peer device beforehand and perform the following configurations:

1. Execute the **public-key peer** command, and then the **public-key-code begin** command to enter public key code view.
2. Type the peer public key.
3. Execute the **public-key-code end** command to save the public key and return to public key view.
4. Execute the **peer-public-key end** command to return to system view.

Related commands: **public-key-code begin**, **public-key-code end**, **peer-public-key end**, and **display public-key peer**.

Examples

# Specify the name for the per public key as **key1** and enter public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key]
```

public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

View

System view

Default level

2: System level

Parameters

keyname: Specifies a public key name, a case-sensitive string of 1 to 64 characters.

filename: Specifies the name of the file that saves the peer host public key. For more information about file name, see *Fundamentals Configuration Guide.*

Description

Use **public-key peer import sshkey** to import a peer host public key from the public key file.

Use **undo public-key peer** to remove the specified peer host public key.

After execution of this command, the system automatically transforms the host public key in SSH1, SSH2.0 or OpenSSH format to PKCS format, and imports the key. This operation requires that you get a copy of the public key file from the peer device through FTP or TFTP in binary mode in advance.

Related commands: **display public-key peer**.

Examples

# Import the peer host public key named **key2** from the public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

PKI configuration commands

attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute { *id* | **all** }

View

Certificate attribute group view

Default level

2: System level

Parameters

id: Sequence number of the certificate attribute rule, in the range of 1 to 16.

alt-subject-name: Specifies the name of the alternative certificate subject.

fqdn: Specifies the FQDN of the entity.

ip: Specifies the IP address of the entity.

issuer-name: Specifies the name of the certificate issuer.

subject-name: Specifies the name of the certificate subject.

dn: Specifies the distinguished name of the entity.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

all: Specifies all certificate attributes.

Description

Use **attribute** to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use **undo attribute** to delete the attribute rules of certificates.

By default, no restriction exists on the issuer name, subject name, and alternative subject name of a certificate.

The attribute of the alternative certificate subject name does not appear as a distinguished name, and therefore the **dn** keyword is not available for the attribute.

Examples

# Create a certificate attribute rule, specifying that the DN in the subject name includes the string of **abc**.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

# Create a certificate attribute rule, specifying that the FQDN in the issuer name cannot be the string of abc.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

# Create a certificate attribute rule, specifying that the IP address in the alternative subject name cannot be 10.0.0.1.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

ca identifier

Syntax

ca identifier *name*

undo ca identifier

View

PKI domain view

Default level

2: System level

Parameters

name: Name of the trusted CA, a case-insensitive string of 1 to 63 characters.

Description

Use **ca identifier** to specify the trusted CA and bind the switch with the CA.

Use **undo ca identifier** to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

Examples

# Specify the trusted CA as **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

View

PKI domain view

Default level

2: System level

Parameters

entity-name: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

Description

Use **certificate request entity** to specify the entity for certificate request.

Use **undo certificate request entity** to remove the configuration.

By default, no entity is specified for certificate request.

Related commands: **pki entity**.

Examples

# Specify the entity for certificate request as **entity1**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request entity entity1
```

certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

View

PKI domain view

Default level

2: System level

Parameters

ca: Indicates that the entity requests a certificate from a CA.

ra: Indicates that the entity requests a certificate from an RA.

Description

Use **certificate request from** to specify the authority for certificate request.

Use **undo certificate request from** to remove the configuration.

By default, no authority is specified for certificate request.

Examples

# Specify that the entity requests a certificate from the CA.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] * | **manual** }

undo certificate request mode

View

PKI domain view

Default level

2: System level

Parameters

auto: Requests certificates in auto mode.

key-length: Length of the RSA keys in bits, in the range of 512 to 2048. It is 1024 bits by default.

cipher: Sets a ciphertext password for certificate revocation.

simple: Sets a plaintext password for certificate revocation.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 31 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters.

manual: Requests certificates in manual mode.

Description

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate. However, if the certificate will expire or has expired, the entity does not initiate a re-request automatically. To have a new local certificate, you need to request one manually. In manual mode, all operations associated with certificate request are carried out manually. The plaintext password or ciphertext password is saved in cipher text in the configuration file.

Related commands: **pki request-certificate**.

Examples

# Specify to request a certificate in auto mode.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *minutes* }

undo certificate request polling { **count** | **interval** }

View

PKI domain view

Default level

2: System level

Parameters

count *count*: Specifies the maximum number of attempts to poll the status of the certificate request, in the range of 1 to 100.

interval *minutes*: Specifies the polling interval in minutes, in the range of 5 to 168.

Description

Use **certificate request polling** to specify the certificate request polling interval and attempt limit.

Use **undo certificate request polling** to restore the defaults.

By default, the polling is executed every 20 minutes for up to 50 times.

After an applicant makes a certificate request, the CA might need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related commands: **display pki certificate**.

Examples

# Specify the polling interval as 15 minutes and the maximum number of attempts as 40.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

Default level

2: System level

Parameters

url-string: URL for certificate request, a case-insensitive string of 1 to 127 characters. It comprises the location of the server and the location of CGI command interface script in the format http://*server_location/ca_script_location*, where *server_location* must be an IP address and does not support domain name resolution.

Description

Use **certificate request url** to specify the URL for certificate request through SCEP.

Use **undo certificate request url** to remove the configuration.

By default, no certificate request URL is specified for a PKI domain.

Examples

# Specify the certificate request URL.

```
<Sysname> system-view
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

Default level

2: System level

Parameters

name: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **common-name** to configure the common name of an entity, which can be, for example, the user name.

Use **undo common-name** to remove the configuration.

By default, no common name is specified.

Examples

# Configure the common name of an entity as **test**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] common-name test
```

country

Syntax

country *country-code-str*

undo country

View

PKI entity view

Default level

2: System level

Parameters

country-code-str: Country code for the entity, a 2-character case-insensitive string.

Description

Use **country** to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use **undo country** to remove the configuration.

By default, no country code is specified.

Examples

# Set the country code of an entity to **CN**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

crl check

Syntax

crl check { **disable** | **enable** }

View

PKI domain view

Default level

2: System level

Parameters

disable: Disables CRL checking.

enable: Enables CRL checking.

Description

Use **crl check** to enable or disable CRL checking.

By default, CRL checking is enabled.

CRLs are files issued by the CA to publish all certificates that have been revoked. Revocation of a certificate might occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

Examples

# Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

crl update-period

Syntax

crl update-period *hours*

undo crl update-period

View

PKI domain view

Default level

2: System level

Parameters

hours: CRL update period in hours, in the range of 1 to 720.

Description

Use **crl update-period** to set the CRL update period, the interval at which a PKI entity with a certificate downloads the latest CRL from the LDAP server.

Use **undo crl update-period** to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

Examples

# Set the CRL update period to 20 hours.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

Default level

2: System level

Parameters

url-string: URL of the CRL distribution point, a case-insensitive string of 1 to 127 characters in the format ldap://*server_location* or http://*server_location*, where *server_location* must be an IP address and does not support domain name resolution.

Description

Use **crl url** to specify the URL of the CRL distribution point.

Use **undo crl url** to remove the configuration.

By default, no CRL distribution point URL is specified.

When the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.

Examples

# Specify the URL of the CRL distribution point.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0.30
```

display pki certificate

Syntax

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

ca: Displays the CA certificate.

local: Displays the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

request-status: Displays the status of a certificate request.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate** to display the contents or request status of a certificate.

Related commands: **certificate request polling**, **pki domain**, and **pki retrieval-certificate**.

Examples

# Display the local certificate.

```
<Sysname> display pki certificate local domain 1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@aabbcc.net
            C=CN
            ST=Country A
            L=City X
            O=abc
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2012 GMT
            Not After : Jan 20 09:07:21 2012 GMT
        Subject:
            C=CN
            ST=Country B
            L=City Y
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00D41D1F …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS: hyf.xxyyzz.net
            X509v3 CRL Distribution Points:
            URI:http://1.1.1.1:447/myca.crl
            …           …
    Signature Algorithm: md5WithRSAEncryption
        A3A5A447 4D08387D …
```

Table 29 Command output

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of the X.509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X.509 (version 3) CRLs

display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a string of 1 to 16 characters.

all: Specifies all certificate attribute-based access control policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate access-control-policy** to display information about certificate attribute-based access control policies.

Examples

# Display information about the certificate attribute-based access control policy named **mypolicy**.

```
<Sysname> display pki certificate access-control-policy mypolicy
 access-control-policy name: mypolicy
     rule  1 deny    mygroup1
     rule  2 permit  mygroup2
```

Table 30 Command output

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy
rule number	Number of the access control rule

display pki certificate attribute-group

Syntax

display pki certificate attribute-group { *group-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-name: Name of a certificate attribute group, a string of 1 to 16 characters.

all: Specifies all certificate attribute groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Examples

# Display information about certificate attribute group mygroup.

```
<Sysname> display pki certificate attribute-group mygroup
 attribute group name: mygroup
      attribute  1 subject-name     dn    ctn   abc
      attribute  2 issuer-name      fqdn  nctn  app
```

Table 31 Command output

Field	Description
attribute group name	Name of the certificate attribute group
attribute *number*	Number of the attribute rule
subject-name	Name of the certificate subject
dn	DN of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

display pki crl domain

Syntax

display pki crl domain *domain-name* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki crl domain** to display the locally saved CRLs.

Related commands: **pki domain** and **pki retrieval-crl**.

Examples

# Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=CN
            O=abc
            OU=soft
            CN=A Test Root
        Last Update: Jan  5 08:44:19 2012 GMT
        Next Update: Jan  5 21:42:13 2012 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
            Revoked Certificates:
            Serial Number: 05a234448E…
            Revocation Date: Feb 6 12:33:22 2012 GMT
            CRL entry extensions:…
            Serial Number: 05a278445E…
            Revocation Date: Feb 7 12:33:22 2012 GMT
            CRL entry extensions:…
```

Table 32 Command output

Field	Description
Version	Version of the CRL
Signature Algorithm	Signature algorithm used by the CRLs
Issuer	CA issuing the CRLs
Last Update	Last update time
Next Update	Next update time
CRL extensions	Extensions of CRL
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X.509 v3.
keyid	ID of the public key A CA might have multiple key pairs. This field indicates the key pair used by the CRL's signature.
Revoked Certificates	Revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Revocation date of the certificate

fqdn

Syntax

fqdn *name-str*

undo fqdn

View

PKI entity view

Default level

2: System level

Parameters

name-str: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 127 characters.

Description

Use **fqdn** to configure the FQDN of an entity.

Use **undo fqdn** to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

Examples

# Configure the FQDN of an entity as **pki.domain-name.com**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

ip (PKI entity view)

Syntax

ip *ip-address*

undo ip

View

PKI entity view

Default level

2: System level

Parameters

ip-address: IP address for an entity.

Description

Use **ip** to configure the IP address of an entity.

Use **undo ip** to remove the configuration.

By default, no IP address is specified for an entity.

Examples

# Configure the IP address of an entity as 11.0.0.1.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

ldap-server

Syntax

ldap-server ip *ip-address* [**port** *port-number*] [**version** *version-number*]

undo ldap-server

View

PKI domain view

Default level

2: System level

Parameters

ip-address: IP address of the LDAP server, in dotted decimal format.

port-number: Port number of the LDAP server, in the range of 1 to 65535. The default is 389.

version-number: LDAP version number, either 2 or 3. By default, it is 2.

Description

Use **ldap-server** to specify an LDAP server for a PKI domain.

Use **undo ldap-server** to remove the configuration.

By default, no LDP server is specified for a PKI domain.

Examples

# Specify an LDAP server for PKI domain 1.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

locality

Syntax

locality *locality-name*

undo locality

View

PKI entity view

Default level

2: System level

Parameters

locality-name: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **locality** to configure the geographical locality of an entity, which can be, for example, a city name.

Use **undo locality** to remove the configuration.

By default, no geographical locality is specified for an entity.

Examples

# Configure the locality of an entity as **city**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

organization

Syntax

organization *org-name*

undo organization

View

PKI entity view

Default level

2: System level

Parameters

org-name: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **organization** to configure the name of the organization to which the entity belongs.

Use **undo organization** to remove the configuration.

By default, no organization name is specified for an entity.

Examples

# Configure the name of the organization to which an entity belongs as **test-lab**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization test-lab
```

organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

View

PKI entity view

Default level

2: System level

Parameters

org-unit-name: Organization unit name for distinguishing different units in an organization, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **organization-unit** to specify the name of the organization unit to which this entity belongs.

Use **undo organization-unit** to remove the configuration.

By default, no organization unit name is specified for an entity.

Examples

# Configure the name of the organization unit to which an entity belongs as **group1**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit group1
```

pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be a, al, or all.

all: Specifies all certificate attribute-based access control policies.

Description

Use **pki certificate access-control-policy** to create a certificate attribute-based access control policy and enter its view.

Use **undo pki certificate access-control-policy** to remove certificate attribute-based access control policies.

No access control policy exists by default.

Examples

# Configure an access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

View

System view

Default level

2: System level

Parameters

group-name: Name for the certificate attribute group, a case-insensitive string of 1 to 16 characters. It cannot be a, al, or all.

all: Specifies all certificate attribute groups.

Description

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view.

Use **undo pki certificate attribute-group** to delete certificate attribute groups.

By default, no certificate attribute group exists.

Examples

# Create a certificate attribute group named **mygroup** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

pki delete-certificate

Syntax

pki delete-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default level

2: System level

Parameters

ca: Deletes the locally stored CA certificate.

local: Deletes the locally stored local certificate.

domain-name: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

Description

Use **pki delete-certificate** to delete the certificate locally stored for a PKI domain.

Examples

# Delete the local certificate for PKI domain **cer**.

```
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

Default level

2: System level

Parameters

domain-name: PKI domain name, a case-insensitive string of 1 to 15 characters.

Description

Use **pki domain** to create a PKI domain and enter PKI domain view.

Use **undo pki domain** to remove a PKI domain.

By default, no PKI domain exists.

Examples

# Create a PKI domain and enter its view.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

Default level

2: System level

Parameters

entity-name: Name for the entity, a case-insensitive string of 1 to 15 characters.

Description

Use **pki entity** to create a PKI entity and enter its view.

Use **undo pki entity** to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

Examples

# Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

pki import-certificate

Syntax

pki import-certificate { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

View

System view

Default level

2: System level

Parameters

ca: Specifies the CA certificate.

local: Specifies the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

der: Specifies the certificate format of DER.

p12: Specifies the certificate format of P12.

pem: Specifies the certificate format of PEM.

filename *filename*: Specifies the name of the certificate file, a case-insensitive string of 1 to 127 characters. It defaults to *domain-name*_ca.cer or *domain-name*_local.cer, the name for the file to be created to save the imported certificate.

Description

Use **pki import-certificate** to import a CA certificate or local certificate from a file and save it locally.

Related commands: **pki domain**.

Examples

# Import the CA certificate for PKI domain **cer** in the PEM format.

```
<Sysname> system-view
[Sysname] pki import-certificate ca domain cer pem
```

pki request-certificate domain

Syntax

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

View

System view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain name, a string of 1 to 15 characters.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

pkcs10: Displays the BASE64-encoded PKCS#10 certificate request information, which can be used to request a certification by an out-of-band means, like phone, disk, or email.

filename *filename*: Specifies the name of the local file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

Description

Use **pki request-certificate domain** to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to print the request information in BASE64 format, or use the **pkcs10 filename** *filename* option to save the request information to a local file and send the file to the CA by an out-of-band means.

This operation will not be saved in the configuration file.

Related commands: **pki domain**.

Examples

# Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END CERTIFICATE REQUEST-----
```

pki retrieval-certificate

Syntax

pki retrieval-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default level

2: System level

Parameters

ca: Retrieves the CA certificate.

local: Retrieves the local certificate.

domain-name: Name of the PKI domain used for certificate request, a string of 1 to 15 characters.

Description

Use **pki retrieval-certificate** to retrieve a certificate from the server for certificate distribution.

Related commands: **pki domain**.

Examples

# Retrieve the CA certificate from the certificate issuing server.

```
<Sysname> system-view
[Sysname] pki retrieval-certificate ca domain 1
```

pki retrieval-crl domain

Syntax

pki retrieval-crl domain *domain-name*

View

System view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use **pki retrieval-crl domain** to retrieve the latest CRLs from the server for CRL distribution.

CRLs help examine the validity of certificates.

Related commands: **pki domain**.

Examples

# Retrieve CRLs.

```
<Sysname> system-view
[Sysname] pki retrieval-crl domain 1
```

pki validate-certificate

Syntax

pki validate-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default level

2: System level

Parameters

ca: Verifies the CA certificate.

local: Verifies the local certificate.

domain-name: Name of the PKI domain to which the certificate to be verified belongs, a string of 1 to 15 characters.

Description

Use **pki validate-certificate** to examine the validity of a certificate.

Certificate validity verification examines whether the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related commands: **pki domain**.

Examples

# Verify the validity of the local certificate.

```
<Sysname> system-view
[Sysname] pki validate-certificate local domain 1
```

root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

View

PKI domain view

Default level

2: System level

Parameters

md5: Uses an MD5 fingerprint.

sha1: Uses a SHA1 fingerprint.

string: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

Description

Use **root-certificate fingerprint** to configure the fingerprint to be used for verifying the validity of the CA root certificate.

Use **undo root-certificate fingerprint** to remove the configuration.

By default, no fingerprint is configured for verifying the validity of the CA root certificate.

Examples

# Configure an MD5 fingerprint for verifying the validity of the CA root certificate.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

# Configure a SHA1 fingerprint for verifying the validity of the CA root certificate.

```
[Sysname-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

rule (PKI CERT ACP view)

Syntax

rule [*id*] { **deny** | **permit** } *group-name*

undo rule { *id* | **all** }

View

PKI certificate access control policy view

Default level

2: System level

Parameters

id: Number of the certificate attribute access control rule, in the range of 1 to 16. The default is the smallest unused number in this range.

deny: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered invalid and denied.

permit: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered valid and permitted.

group-name: Name of the certificate attribute group to be associated with the rule, a case-insensitive string of 1 to 16 characters. It cannot be a, al, or all.

all: Specifies all access control rules.

Description

Use **rule** to create a certificate attribute access control rule.

Use **undo rule** to delete access control rules.

By default, no access control rule exists.

A certificate attribute group must exist to be associated with a rule.

Examples

# Create an access control rule, specifying that a certificate is considered valid when it matches an attribute rule in certificate attribute group mygroup.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

state

Syntax

state *state-name*

undo state

View

PKI entity view

Default level

2: System level

Parameters

state-name: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **state** to specify the name of the state or province where an entity resides.

Use **undo state** to remove the configuration.

By default, no state or province is specified.

Examples

# Specify the state where an entity resides.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] state country
```

SSH2.0 configuration commands

SSH2.0 server configuration commands

display ssh server

Syntax

display ssh server { **session** | **status** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

session: Displays the session information of the SSH server.

status: Displays the status information of the SSH server.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh server** on an SSH server to display SSH server status information or session information.

This command is also available on an SFTP server.

Related commands: **ssh server authentication-retries**, **ssh server authentication-timeout**, **ssh server compatible-ssh1x enable**, **ssh server enable**, and **ssh server rekey-interval**.

Examples

# Display SSH server status information.

```
<Sysname> display ssh server status
 SSH Server: Disable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH Authentication retries : 3 time(s)
 SFTP Server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
```

Table 33 Command output

Field	Description
SSH Server	Whether the SSH server function is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period.
SSH server key generating interval	SSH server key pair update interval.
SSH Authentication retries	Maximum number of authentication attempts for SSH users.
SFTP Server	Whether the SFTP server function is enabled.
SFTP Server Idle-Timeout	SFTP connection idle timeout period.

# Display the SSH server session information.

```
<Sysname> display ssh server session
 Conn    Ver   Encry    State         Retry    SerType  Username
 VTY 0   2.0   DES      Established   0        SFTP     client001
```

Table 34 Command output

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init, Ver-exchange, Keys-exchange, Auth-request, Serv-request, Established, Disconnected
Retry	Number of authentication attempts
SerType	Service type (SCP, SFTP, and Stelnet)
Username	Name of a user for login

display ssh user-information

Syntax

display ssh user-information [*username*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

username: Specifies an SSH username, a string of 1 to 80 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh user-information** on an SSH server to display information about SSH users.

This command displays only information about SSH users configured through the **ssh user** command on the SSH server.

Without the *username* argument, the command displays information about all SSH users.

This command is also available on an SFTP server.

Related commands: **ssh user**.

Examples

# Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users : 2
 Username    Authentication-type   User-public-key-name     Service-type
 yemx        password              null                     all
 test        publickey             pubkey                   sftp
```

Table 35 Command output

Field	Description
Username	Name of the user.
Authentication-type	Authentication method. If this field has a value of **password**, the next field has a value of **null**.
User-public-key-name	Public key of the user.

ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Default level

3: Manage level

Parameters

times: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Description

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

By default, the maximum number of authentication attempts for SSH users is 3.

This configuration takes effect only for the users at next login.

Authentication fails if the total number of authentication attempts (including both publickey and password authentication) exceeds the upper limit configured by the **ssh server authentication-retries** command.

If the authentication method of SSH users is **password-publickey**, the server first uses publickey authentication, and then uses password authentication to authenticate SSH users. The process is regarded as one authentication attempt.

Related commands: **display ssh server**.

Examples

# Set the maximum number of authentication attempts for SSH users to 4.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

View

System view

Default level

3: Manage level

Parameters

time-out-value: Specifies an authentication timeout period in seconds, in the range of 1 to 120.

Description

Use **ssh server authentication-timeout** to set the SSH user authentication timeout period on the SSH server.

Use **undo ssh server authentication-timeout** to restore the default.

By default, the authentication timeout period is 60 seconds.

Related commands: **display ssh server**.

Examples

# Set the SSH user authentication timeout period to 10 seconds.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server compatible-ssh1x

Syntax

ssh server compatible-ssh1x [**enable**]

undo ssh server compatible-ssh1x

View

System view

Default level

3: Manage level

Parameters

enable: Enables the SSH server to support SSH1 clients. This keyword is not necessary. Even if it is not specified, the command can also enable the SSH server to support SSH1 clients.

Description

Use **ssh server compatible-ssh1x** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** to disable the SSH server from supporting SSH1 clients.

By default, the SSH server supports SSH1 clients.

The configuration takes effect only for clients that log in after the configuration

Related commands: **display ssh server**.

Examples

# Enable the SSH server to support SSH1 clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv4 SSH server, which ranges from 0 to 63.

Description

Use **ssh server dscp** to set the DSCP value for packets sent by the IPv4 SSH server.

Use **undo ssh server dscp** to restore the default.

By default, the DSCP value in packets sent by the IPv4 SSH server is 16.

Examples

# Set the DSCP value to 30 for packets sent by the IPv4 SSH server.

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

ssh server enable

Syntax

ssh server enable

undo ssh server enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **ssh server enable** to enable the SSH server function.

Use **undo ssh server enable** to disable the SSH server function.

By default, SSH server is disabled.

Examples

# Enable SSH server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv6 SSH server, which ranges from 0 to 63.

Description

Use **ssh server ipv6 dscp** to set the DSCP value for packets sent by the IPv6 SSH server.

Use **undo ssh server ipv6 dscp** to restore the default.

By default, the DSCP value in packets sent by the IPv6 SSH server is 0.

Examples

# Set the DSCP value to 30 for packets sent by the IPv6 SSH server.

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Default level

3: Manage level

Parameters

hours: Specifies an interval (in hours) for updating the server key pair, in the range of 1 to 24.

Description

Use **ssh server rekey-interval** to set the interval for updating the RSA server key.

Use **undo ssh server rekey-interval** to restore the default.

By default, the update interval of the RSA server key is 0, and the RSA server key is not updated.

This command is only available to SSH users using SSH1 client software.

The system does not update any DSA key pair periodically.

Related commands: **display ssh server**.

Examples

# Set the RSA server key pair update interval to 3 hours.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

ssh user

Syntax

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

View

System view

Default level

3: Manage level

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies Stelnet, SFTP, and SCP.
- **scp**: Specifies the service type as secure copy.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one of the following:

- **password**: Specifies password authentication. This authentication method features easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies either password authentication or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication (featuring higher security) if the client runs SSH2, and performs either type of authentication if the client runs SSH1.
- **publickey**: Specifies publickey authentication. This authentication method has the downside of complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. Once it is configured, the authentication process completes automatically without the need of remembering or entering any password.

assign publickey *keyname*: Assigns an existing public key to an SSH user. The *keyname* argument indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies the working directory for an SFTP user. The *directory-name* argument indicates the name of the working directory and is a string of 1 to 135 characters.

Description

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

For a publickey authentication user, you must configure the username and the public key on the switch. For a password authentication user, you can configure the account information on either the switch or the remote authentication server, such as a RADIUS server.

If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

You can change the authentication method and public key of an SSH user when the user is communicating with the SSH server. However, your changes take effect for the clients at next login.

If an SCP or SFTP user has been assigned a public key, it is necessary to set a working folder for the user.

The working folder of an SCP or SFTP user depends on the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both publickey authentication and password authentication, the working folder is the one set by using the **ssh user** command.

Related commands: **display ssh user-information**.

Examples

# Create an SSH user named **user1**, set the service type as **sftp**, the authentication method as **publickey**, assign a public key named **key1** to the user, and specify the working directory of the SFTP server as **flash**:/.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey
key1 work-directory flash:/
```

SSH2.0 client configuration commands

display ssh client source

Syntax

display ssh client source [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh client source** to display the source IP address or source interface information on an SSH client.

If neither source IP address nor source interface is specified for the SSH client, the system displays the message "Neither source IP address nor source interface was specified for the Stelnet client."

Related commands: **ssh client source**.

Examples

# Display the source IP address or source interface of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

display ssh server-info

Syntax

display ssh server-info [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh server-info** on a client to display mappings between SSH servers and their host public keys on an SSH client.

When an SSH client needs to authenticate the SSH server, it uses the locally saved public key of the server for the authentication. If the authentication fails, you can use this command to check the public key of the server saved on the client.

This command is also available on an SFTP client.

Related commands: **ssh client authentication server**.

Examples

# Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP)                 Server public key name
______________________________________________________
192.168.0.1                      abc_key01
192.168.0.2                      abc_key02
```

Table 36 Command output

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

ssh client authentication server

Syntax

ssh client authentication server *server* **assign publickey** *keyname*

undo ssh client authentication server *server* **assign publickey**

View

System view

Default level

2: System level

Parameters

server: Specifies an IP address or name of the server, a string of 1 to 80 characters.

assign publickey *keyname*: Specifies the name of the host public key of the server, a string of 1 to 64 characters.

Description

Use **ssh client authentication server** on a client to configure the host public key of a server so that the client can determine whether the server is trustworthy.

Use **undo ssh client authentication server** to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

A client that does not support first-time authentication rejects unauthenticated servers. To enable the client to use the correct public key of a server to authenticate the server, you must configure the public keys of the servers and specify the mappings between public keys and servers on the client.

The specified host public key of the server must already exist.

Related commands: **ssh client first-time enable**.

Examples

# Configure the public key of the server with the IP address of 192.168.0.1 to be key1.

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

ssh client dscp

Syntax

ssh client dscp *dscp-value*

undo ssh client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv4 SSH client, which ranges from 0 to 63.

Description

Use **ssh client dscp** to set the DSCP value for packets sent by the IPv4 SSH client.

Use **undo ssh client dscp** to restore the default.

By default, the DSCP value in packets sent by the IPv4 SSH client is 16.

Examples

# Set the DSCP value to 30 for packets sent by the IPv4 SSH client.

```
<Sysname> system-view
[Sysname] ssh client dscp 30
```

ssh client first-time

Syntax

ssh client first-time [**enable**]

undo ssh client first-time

View

System view

Default level

2: System level

Parameters

enable: Enables the first-time authentication of the SSH client to the SSH server. This keyword is not necessary. Even if it is not specified, the command can also enable the first-time authentication function.

Description

Use **ssh client first-time** to enable the first-time authentication function.

Use **undo ssh client first-time** to disable the function.

By default, the function is enabled.

With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client uses the saved server host public key to authenticate the server.

Without first-time authentication, a client that is not configured with the server host public key refuses to access the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Because the server might update its key pairs periodically, clients must obtain the most recent public keys of the server for successful authentication of the server.

Examples

# Enable the first-time authentication function.

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

ssh client ipv6 dscp

Syntax

ssh client ipv6 dscp *dscp-value*

undo ssh client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv6 SSH client, which ranges from 0 to 63.

Description

Use **ssh client ipv6 dscp** to set the DSCP value for packets sent by the IPv6 SSH client.

Use **undo ssh client ipv6 dscp** to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 SSH client is 0.

Examples

# Set the DSCP value to 30 for protocol packets sent by the IPv6 SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 dscp 30
```

ssh client ipv6 source

Syntax

ssh client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo ssh client ipv6 source

View

System view

Default level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **ssh client ipv6 source** to specify the source IPv6 address or source interface for the SSH client.

Use **undo ssh client ipv6 source** to remove the configuration.

By default, an SSH client uses the IPv6 address of the interface specified by the route of the device to access the SSH server.

Related commands: **display ssh client source**.

Examples

# Specify the source IPv6 address as 2:2::2:2 for the SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax

ssh client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo ssh client source

View

System view

Default level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **ssh client source** to specify the source IPv4 address or source interface of the SSH client.

Use **undo ssh client source** to remove the configuration.

By default, an SSH client uses the IP address of the interface specified by the route of the device to access the SSH server.

Related commands: **display ssh client source**.

Examples

# Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

ssh2

Syntax

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default level

0: Visit level

Parameters

server: Specifies an IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Specifies the encryption algorithm 3des-cbc.
- **aes128**: Specifies the encryption algorithm aes128-cbc.
- **des**: Specifies the encryption algorithm des-cbc.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: Specifies the HMAC algorithm hmac-md5.
- **md5-96**: Specifies the HMAC algorithm hmac-md5-96.
- **sha1**: Specifies the HMAC algorithm hmac-sha1.
- **sha1-96**: Specifies the HMAC algorithm hmac-sha1-96.

prefer-kex: Specifies the preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Specifies the key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Specifies the key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Specifies the key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Description

Use **ssh2** to establish a connection to an IPv4 SSH server and specify the publickey algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

When the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the public key algorithm is DSA.

Examples

# Log in to remote SSH2.0 server 10.214.50.51, using the following algorithms:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

ssh2 ipv6

Syntax

ssh2 ipv6 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default level

0: Visit level

Parameters

server: Specifies an IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Specifies the encryption algorithm 3des-cbc.
- **aes128**: Specifies the encryption algorithm aes128-cbc.
- **des**: Specifies the encryption algorithm des-cbc.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: Specifies the HMAC algorithm hmac-md5.
- **md5-96**: Specifies the HMAC algorithm hmac-md5-96.
- **sha1**: Specifies the HMAC algorithm hmac-sha1.
- **sha1-96**: Specifies the HMAC algorithm hmac-sha1-96.

prefer-kex: Specifies the preferred key exchange algorithm, default to **dh-group-exchange**.

- **dh-group-exchange**: Specifies the key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Specifies the key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Specifies the key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Description

Use **ssh2 ipv6** to establish a connection to an IPv6 SSH server and specify publickey algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

When the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the public key algorithm is DSA.

Examples

# Log in to remote SSH2.0 server 2000::1, setting the algorithms as follows:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

SFTP configuration commands

SFTP server configuration commands

sftp server enable

Syntax

sftp server enable

undo sftp server enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **sftp server enable** to enable the SFTP server function.

Use **undo sftp server enable** to disable the SFTP server function.

By default, the SFTP server function is disabled.

Related commands: **display ssh server**.

Examples

# Enable the SFTP server function.

```
<Sysname> system-view
[Sysname] sftp server enable
```

sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

View

System view

Default level

3: Manage level

Parameters

time-out-value: Specifies the timeout period in minutes, in the range of 1 to 35791.

Description

Use **sftp server idle-timeout** to set the idle timeout period for SFTP user connections.

Use **undo sftp server idle-timeout** to restore the default.

By default, the idle timeout period is 10 minutes.

Related commands: **display ssh server**.

Examples

# Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

SFTP client configuration commands

bye

Syntax

bye

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **bye** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **exit** and **quit** commands.

Examples

# Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
Connection closed.
<Sysname>
```

cd

Syntax

cd [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path: Specifies the name of a path on the server.

Description

Use **cd** to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

# Change the working path to **new1**.

```
sftp-client> cd new1
Current Directory is:
/new1
```

cdup

Syntax

cdup

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **cdup** to return to the upper-level directory.

Examples

# From the current working directory /new1, return to the upper-level directory.

```
sftp-client> cdup
Current Directory is:
/
```

delete

Syntax

delete *remote-file*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file&<1-10>: Specifies the names of files on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use **delete** to delete files from a server.

This command functions as the **remove** command.

Examples

# Delete file **temp.c** from the server.

```
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation might take a long time. Please wait...

File successfully Removed
```

dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

-a: Displays the names of the files and sub-directories under the specified directory.

-l: Displays the detailed information of the files and sub-directories under the specified directory in the form of a list.

remote-path: Specifies the name of the directory to be queried.

Description

Use **dir** to display information about the files and sub-directories under a directory.

With the **–a** and **–l** keyword not specified, the command displays detailed information of the files and sub-directories under the specified directory in the form of a list.

With the *remote-path* not specified, the command displays information about the files and sub-directories of the current working directory.

This command functions as the **ls** command.

Examples

# Display detailed information about the files and sub-directories under the current working directory in the form of a list.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
```

```
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

display sftp client source

Syntax

display sftp client source [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display sftp client source** to display the source IP address or source interface set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, the system displays the message "Neither source IP address nor source interface was specified for the SFTP client."

Related commands: **sftp client source**.

Examples

# Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

exit

Syntax

exit

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **exit** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **quit** commands.

Examples

# Terminate the connection with the remote SFTP server.

```
sftp-client> exit
Bye
Connection closed.
<Sysname>
```

get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file: Name of a file on the remote SFTP server.

local-file: Name for the local file.

Description

Use **get** to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

Examples

# Download file **temp1.c** and save it as **temp.c** locally.

```
sftp-client> get temp1.c temp.c
Remote  file:/temp1.c --->  Local file: temp.c
Downloading file successfully ended
```

help

Syntax

help [**all** | *command-name*]

View

SFTP client view

Default level

3: Manage level

Parameters

all: Displays a list of all commands.

command-name: Specifies the name of a command.

Description

Use **help** to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Examples

# Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file.Default local-path is the same
                              as remote-path
```

ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

-a: Displays the filenames and the folder names of the specified directory.

-l: Displays in a list form detailed information of the files and folders of the specified directory.

remote-path: Name of the directory to be queried.

Description

Use **ls** to display file and folder information under a directory.

With the **–a** and **–l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Examples

# Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path: Specifies the name for the directory on a remote SFTP server.

Description

Use **mkdir** to create a directory on a remote SFTP server.

Examples

# Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

Default level

3: Manage level

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name for the file on a remote SFTP server.

Description

Use **put** to upload a local file to a remote SFTP server.

If the *remote-file* argument is not specified, the file will be saved remotely with the same name as the local one.

Examples

# Upload local file **temp.c** to the remote SFTP server and save it as **temp1.c**.

```
sftp-client> put temp.c temp1.c
Local file:temp.c --->  Remote file: /temp1.c
Uploading file successfully ended
```

pwd

Syntax

pwd

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **pwd** to display the current working directory of a remote SFTP server.

Examples

# Display the current working directory of the remote SFTP server.

```
sftp-client> pwd
/
```

quit

Syntax

quit

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **quit** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **exit** commands.

Examples

# Terminate the connection with the remote SFTP server.

```
sftp-client> quit
Bye
Connection closed.
<Sysname>
```

remove

Syntax

remove *remote-file*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file&<1-10>: Specifies names of files on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use **remove** to delete files from a remote server.

This command functions as the **delete** command.

Examples

# Delete file temp.c from the server.

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation might take a long time.Please wait...

File successfully Removed
```

rename

Syntax

rename *oldname newname*

View

SFTP client view

Default level

3: Manage level

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies the new name for the file or directory.

Description

Use **rename** to change the name of a file or directory on an SFTP server.

Examples

# Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

rmdir

Syntax

rmdir *remote-path*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path&<1-10>: Specifies the names of directories on the remote SFTP server. &<1-10> means that you can provide up to 10 directory names that are separated by space.

Description

Use **rmdir** to delete the specified directories from an SFTP server.

Examples

# On the SFTP server, delete directory **temp1** in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

sftp

Syntax

sftp *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default level

3: Manage level

Parameters

server: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is dsa.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Specifies the encryption algorithm 3des-cbc.
- **aes128**: Specifies the encryption algorithm aes128-cbc.
- **des**: Specifies the encryption algorithm des-cbc.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: Specifies the HMAC algorithm hmac-md5.
- **md5-96**: Specifies the HMAC algorithm hmac-md5-96.

- **sha1**: Specifies the HMAC algorithm hmac-sha1.
- **sha1-96**: Specifies the HMAC algorithm hmac-sha1-96.

prefer-kex: Specifies the preferred key exchange algorithm, defaulted to dh-group-exchange.

- **dh-group-exchange**: Specifies the key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Specifies the key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Specifies the key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client, defaulted to aes128.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Description

Use **sftp** to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

When the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the public key algorithm is DSA.

Examples

# Connect to SFTP server 10.1.1.2, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
Input Username:
```

sftp client dscp

Syntax

sftp client dscp *dscp-value*

undo sftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv4 SFTP client, which ranges from 0 to 63.

Description

Use **sftp client dscp** to set the DSCP value for packets sent by the IPv4 SFTP client.

Use **undo sftp client dscp** to restore the default.

By default, the DSCP value in packets sent by the IPv4 SFTP client is 16.

Examples

# Set the DSCP value to 30 for packets sent by the IPv4 SFTP client.

```
<Sysname> system-view
[Sysname] sftp client dscp 30
```

sftp client ipv6 dscp

Syntax

sftp client ipv6 dscp *dscp-value*

undo sftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the packets sent by the IPv6 SFTP client, which ranges from 0 to 63.

Description

Use **sftp client ipv6 dscp** to set the DSCP value for packets sent by the IPv6 SFTP client.

Use **undo sftp client ipv6 dscp** to restore the default.

By default, the DSCP value in packets sent by the IPv6 SFTP client is 8.

Examples

# Set the DSCP value to 30 for packets sent by the IPv6 SFTP client.

```
<Sysname> system-view
[Sysname] sftp client ipv6 dscp 30
```

sftp client ipv6 source

Syntax

sftp client ipv6 source { **ipv6** ipv6-address | **interface** interface-type interface-number }

undo sftp client ipv6 source

View

System view

Default level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **sftp client ipv6 source** to specify the source IPv6 address or source interface for an SFTP client.

Use **undo sftp client ipv6 source** to remove the configuration.

By default, an SFTP client uses the IPv6 address of the interface specified by the route of the device to access the SFTP server.

Related commands: **display sftp client source**.

Examples

# Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

sftp client source

Syntax

sftp client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo sftp client source

View

System view

Default level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **sftp client source** to specify the source IPv4 address or interface of an SFTP client.

Use **undo sftp client source** to remove the configuration.

By default, an SFTP client uses the IP address of the interface specified by the route of the device to access the SFTP server.

Related commands: **display sftp client source**.

Examples

# Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

sftp ipv6

Syntax

sftp ipv6 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default level

3: Manage level

Parameters

server: Specifies an IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Specifies the encryption algorithm 3des-cbc.
- **aes128**: Specifies the encryption algorithm aes128-cbc.
- **des**: Specifies the encryption algorithm des-cbc.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: Specifies the HMAC algorithm hmac-md5.
- **md5-96**: Specifies the HMAC algorithm hmac-md5-96.
- **sha1**: Specifies the HMAC algorithm hmac-sha1.
- **sha1-96**: Specifies the HMAC algorithm hmac-sha1-96.

prefer-kex: Specifies the preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Specifies the key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Specifies the key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Specifies the key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Description

Use **sftp ipv6** to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

When the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the public key algorithm is DSA.

Examples

# Connect to server 2:5::8:9, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
Input Username:
```

SCP configuration commands

SCP client configuration commands

scp

Command

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default level

3: Manage level

Parameters

ipv6: Specifies the type of the server as IPv6. If this keyword is not specified, the server is an IPv4 server.

server: Specifies an IPv4 or IPv6 address or host name of the server, a case-insensitive string of 1 to 255 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

- **dsa**: Specifies the public key algorithm **dsa.**
- **rsa**: Specifies the public key algorithm **rsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Specifies the encryption algorithm 3des-cbc.
- **aes128**: Specifies the encryption algorithm aes128-cbc.
- **des**: Specifies the encryption algorithm des-cbc.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: Specifies the HMAC algorithm hmac-md5.
- **md5-96**: Specifies the HMAC algorithm hmac-md5-96.
- **sha1**: Specifies the HMAC algorithm hmac-sha1.
- **sha1-96**: Specifies the HMAC algorithm hmac-sha1-96.

prefer-kex: Specifies the preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Specifies the key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Specifies the key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Specifies the key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Description

Use **scp** to transfer files with an SCP server.

When the client's authentication method is publickey, the client needs to get the local private key for digital signature. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the public key algorithm is DSA.

Examples

# Download the file **remote.bin** from the SCP server, save it locally and change the file name to **local.bin**

```
<Sysname> scp 192.168.0.1 get remote.bin local.bin
```

SSL configuration commands

ciphersuite

Syntax

ciphersuite [**rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] *

View

SSL server policy view

Default level

2: System level

Parameters

rsa_3des_ede_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use **ciphersuite** to specify the cipher suites for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.

If you execute the command repeatedly, the last one takes effect.

Related commands: **display ssl server-policy**.

Examples

# Configure SSL server policy policy1 to support cipher suites **rsa_rc4_128_md5** and **rsa_rc4_128_sha**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

client-verify enable

Syntax

client-verify enable

undo client-verify enable

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **client-verify enable** to configure the SSL server to require the client to pass certificate-based authentication.

Use **undo client-verify enable** to restore the default.

By default, the SSL server does not require certificate-based SSL client authentication.

If you configure the **client-verify enable** command and enable the SSL client weak authentication function, whether the client must be authenticated is up to the client. If the client chooses to be authenticated, the client must pass authentication before accessing the SSL server; otherwise, the client can access the SSL server without authentication.

If you configure the **client-verify enable** command but disable the SSL client weak authentication function, the SSL client must pass authentication before accessing the SSL server.

Related commands: **client-verify weaken** and **display ssl server-policy**.

Examples

# Configure the SSL server to require certificate-based SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

client-verify weaken

Syntax

client-verify weaken

undo client-verify weaken

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **client-verify weaken** to enable SSL client weak authentication.

Use **undo client-verify weaken** to restore the default.

By default, SSL client weak authentication is disabled.

If the SSL server requires certificate-based client authentication and the SSL client weak authentication function is enabled, whether the client must be authenticated is up to the client. If the client chooses to be authenticated, the client must pass authentication before accessing the SSL server; otherwise, the client can access the SSL server without authentication.

If the SSL server requires certificate-based client authentication and SSL client weak authentication is disabled, the SSL client must pass authentication before accessing the SSL server.

NOTE:

The **client-verify weaken** command takes effect only when the SSL server requires certificate-based client authentication.

Related commands: **client-verify enable** and **display ssl server-policy**.

Examples

# Enable SSL client weak authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
[Sysname-ssl-server-policy-policy1] client-verify weaken
```

close-mode wait

Syntax

close-mode wait

undo close-mode wait

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **close-mode wait** to set the SSL connection close mode to wait mode. In this mode, after sending a close-notify alert message to a client, the server does not close the connection until it receives a close-notify alert message from the client.

Use **undo close-mode wait** to restore the default.

By default, an SSL server sends a close-notify alert message to the client and closes the connection without waiting for the close-notify alert message from the client.

Related commands: **display ssl server-policy**.

Examples

# Set the SSL connection close mode to **wait**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

display ssl client-policy

Syntax

display ssl client-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL client policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssl client-policy** to display information about SSL client policies.

Examples

# Display information about SSL client policy **policy1**.

```
<Sysname> display ssl client-policy policy1
 SSL Client Policy: policy1
     SSL Version: SSL 3.0
     PKI Domain: 1
     Prefer Ciphersuite:
         RSA_RC4_128_SHA
     Server-verify: enabled
```

Table 37 Command output

Field	Description
SSL Client Policy	SSL client policy name
SSL Version	Version of the protocol used by the SSL client policy, SSL 3.0 or TLS 1.0
PKI Domain	PKI domain of the SSL client policy
Prefer Ciphersuite	Preferred cipher suite of the SSL client policy

Field	Description
Server-verify	Whether server authentication is enabled for the SSL client policy

display ssl server-policy

Syntax

display ssl server-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL server policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssl server-policy** to display information about SSL server policies.

Examples

# Display information about SSL server policy **policy1**.

```
<Sysname> display ssl server-policy policy1
 SSL Server Policy: policy1
     PKI Domain: domain1
     Ciphersuite:
         RSA_RC4_128_MD5
         RSA_RC4_128_SHA
         RSA_DES_CBC_SHA
         RSA_3DES_EDE_CBC_SHA
         RSA_AES_128_CBC_SHA
         RSA_AES_256_CBC_SHA
     Handshake Timeout: 3600
     Close-mode: wait disabled
     Session Timeout: 3600
     Session Cachesize: 500
     Client-verify: disabled
     Client-verify weaken: disabled
```

Table 38 Command output

Field	Description
SSL Server Policy	SSL server policy name.
PKI Domain	PKI domain used by the SSL server policy.
Ciphersuite	Cipher suites supported by the SSL server policy.
Handshake Timeout	Handshake timeout time of the SSL server policy, in seconds.
Close-mode	Close mode of the SSL server policy: • **wait disabled**—In this mode, the server sends a close-notify alert message to the client and then closes the connection immediately without waiting for the close-notify alert message of the client. • **wait enabled**—In this mode, the server sends a close-notify alert message to the client and then waits for the close-notify alert message of the client. Only after receiving the expected message, does the server close the connection.
Session Timeout	Session timeout time of the SSL server policy, in seconds.
Session Cachesize	Maximum number of buffered sessions of the SSL server policy.
Client-verify	Whether the SSL server policy requires the client to be authenticated.

handshake timeout

Syntax

handshake timeout *time*

undo handshake timeout

View

SSL server policy view

Default level

2: System level

Parameters

time: Handshake timeout time in seconds, in the range of 180 to 7200.

Description

Use **handshake timeout** to set the handshake timeout time for an SSL server policy.

Use **undo handshake timeout** to restore the default.

By default, the handshake timeout time is 3600 seconds.

If the SSL server does not receive any packet from the SSL client before the handshake timeout time expires, the SSL server will terminate the handshake process.

Related commands: **display ssl server-policy**.

Examples

# Set the handshake timeout time of SSL server policy policy1 to 3000 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view, SSL client policy view

Default level

2: System level

Parameters

domain-name: Name of a PKI domain, a case-insensitive string of 1 to 15 characters.

Description

Use **pki-domain** to specify a PKI domain for an SSL server policy or SSL client policy.

Use **undo pki-domain** to restore the default.

By default, no PKI domain is configured for an SSL server policy or SSL client policy.

Related commands: **display ssl server-policy** and **display ssl client-policy**.

Examples

# Configure SSL server policy policy1 to use PKI domain **server-domain**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

# Configure SSL client policy policy1 to use PKI domain **client-domain**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

prefer-cipher

Syntax

prefer-cipher { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

View

SSL client policy view

Default level

2: System level

Parameters

rsa_3des_ede_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use **prefer-cipher** to specify the preferred cipher suite for an SSL client policy.

Use **undo prefer-cipher** to restore the default.

By default, the preferred cipher suite for an SSL client policy is **rsa_rc4_128_md5**.

Related commands: **display ssl client-policy**.

Examples

# Set the preferred cipher suite for SSL client policy policy1 to **rsa_aes_128_cbc_sha**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

server-verify enable

Syntax

server-verify enable

undo server-verify enable

View

SSL client policy view

Default level

2: System level

Parameters

None

Description

Use **server-verify enable** to enable certificate-based SSL server authentication so that the SSL client authenticates the server by the server's certificate during the SSL handshake process.

Use **undo server-verify enable** to disable certificate-based SSL server authentication. When certificate-based SSL server authentication is disabled, it is assumed that the SSL server is valid.

By default, certificate-based SSL server authentication is enabled.

Related commands: **display ssl client-policy**.

Examples

# Enable certificate-based SSL server authentication.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

session

Syntax

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

View

SSL server policy view

Default level

2: System level

Parameters

cachesize *size*: Specifies the maximum number of cached sessions, in the range of 100 to 1000.

timeout *time*: Specifies the caching timeout time in seconds, in the range of 1800 to 72000.

Description

Use **session** to set the maximum number of cached sessions and the caching timeout time.

Use **undo session** to restore the default.

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3600 seconds.

It is a complicated process to use the SSL handshake protocol to negotiate session parameters and establish sessions. To simplify the process, SSL allows reusing negotiated session parameters to establish sessions. This feature requires that the SSL server maintain information about existing sessions.

The number of cached sessions and the session information caching time are limited:

- If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions.
- If a session has been cached for a period equal to the caching timeout time, SSL will remove the information of the session.

Related commands: **display ssl server-policy**.

Examples

# Set the caching timeout time to 4000 seconds and the maximum number of cached sessions to 600.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

ssl client-policy

Syntax

ssl client-policy *policy-name*

undo ssl client-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters, which cannot be **a**, **al**, or **all**.

all: Specifies all SSL client policies.

Description

Use **ssl client-policy** to create an SSL policy and enter its view.

Use **undo ssl client-policy** to delete SSL client policies.

Related commands: **display ssl client-policy**.

Examples

# Create SSL client policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be "a", "al", or "all".

all: Specifies all SSL server policies.

Description

Use **ssl server-policy** to create an SSL server policy and enter its view.

Use **undo ssl server-policy** to delete SSL server policies.

You cannot delete an SSL server policy that has been associated with one or more application layer protocols.

Related commands: **display ssl server-policy**.

Examples

# Create SSL server policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

version

Syntax

version { **ssl3.0** | **tls1.0** }

undo version

View

SSL client policy view

Default level

2: System level

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

Description

Use **version** to specify the SSL protocol version for an SSL client policy.

Use **undo version** to restore the default.

By default, the SSL protocol version for an SSL client policy is TLS 1.0.

Related commands: **display ssl client-policy**.

Examples

# Specify the SSL protocol version for SSL client policy policy1 as SSL 3.0.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version ssl3.0
```

TCP attack protection configuration commands

display tcp status

Syntax

display tcp status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp status** to display status of all TCP connections for monitoring TCP connections.

Examples

# Display status of all TCP connections.

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB          Local Add:port        Foreign Add:port      State
03e37dc4       0.0.0.0:4001          0.0.0.0:0             Listening
04217174       100.0.0.204:23        100.0.0.253:65508     Established
```

Table 39 Command output

Field	Description
*: TCP MD5 Connection	If the status information of a TCP connection contains an asterisk (*), the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block.
Local Add:port	Local IP address and port number.
Foreign Add:port	Remote IP address and port number.
State	State of the TCP connection.

tcp syn-cookie enable

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **tcp syn-cookie enable** to enable the SYN Cookie feature to protect the device against SYN Flood attacks.

Use **undo tcp syn-cookie enable** to disable the SYN Cookie feature.

By default, the SYN Cookie feature is enabled.

Examples

# Enable the SYN Cookie feature.

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

IP source guard configuration commands

display ip source binding

Syntax

display ip source binding [**static**] [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

static: Displays static IPv4 source guard entries, including global static IPv4 binding entries and port-based static IPv4 binding entries. If you do not specify this keyword, the command displays all static and dynamic IPv4 source guard entries.

interface *interface-type interface-number*: Displays IPv4 source guard entries of the interface specified by its type and number.

ip-address *ip-address*: Displays IPv4 source guard entries of an IP address.

mac-address *mac-address*: Displays IPv4 source guard entries of an MAC address (in the format H-H-H).

slot *slot-number*: Displays IPv4 source guard entries on an IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip source binding** to display IPv4 source guard entries.

Note the following when you do not use the **static** keyword: If you do not specify any other parameters either, the command displays static and dynamic IPv4 binding entries on all ports and the global static IPv4 binding entries on the master device.

Note the following when you use the **static** keyword: If you do not specify any other parameters, the command displays all global and port-based static IPv4 binding entries.

Related commands: **ip verify source** and **ip source binding**.

Examples

# Display all IPv4 source guard entries.

```
<Sysname> display ip source binding
Total entries found: 3
 MAC Address          IP Address          VLAN       Interface       Type
 040a-0000-4000       10.1.0.9            N/A        GE1/0/1         Static
 040a-0000-3000       10.1.0.8            2          GE1/0/2         DHCP-SNP
 040a-0000-2000       10.1.0.7            2          GE1/0/2         DHCP-SNP
```

# Display all static IPv4 source guard entries.

```
<Sysname> display ip source binding static
Total entries found: 3
 MAC Address           IP Address         VLAN       Interface       Type
 040a-0000-0011        10.1.1.11          N/A        N/A             Static
 040a-0000-0012        10.1.0.12          N/A        GE1/0/3         Static
 040a-0000-0013        10.1.0.13          N/A        GE1/0/3         Static
```

Table 40 Command output

Field	Description
Total entries found	Total number of found entries
MAC Address	MAC address of the IP source guard entry. N/A means that no MAC address is bound in the entry.
IP Address	IP address of the IP source guard entry. N/A means that no IP address is bound in the entry.
VLAN	VLAN bound to the IP source guard entry. N/A means that no VLAN information exists in the entry.
Interface	Interface of the IPv4 source guard entry
Type	Type of the IPv4 source guard entry: • **Static**—Static IPv4 binding entry • **DHCP-SNP**—Entry generated based on DHCP snooping entry • **DHCP-RLY**—Entry generated based on DHCP relay entry

display ipv6 source binding

Syntax

display ipv6 source binding [**static**] [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

static: Displays static IPv6 source guard entries, including global static IPv6 binding entries and port-based static IPv6 binding entries. If you do not specify this keyword, the command displays all static and dynamic IPv6 source guard entries.

interface *interface-type interface-number*: Displays the IPv6 source guard entries of an interface.

ipv6-address *ipv6-address*: Displays the IPv6 source guard entries of an IPv6 address.

mac-address *mac-address*: Displays the IPv6 source guard entries of an MAC address. The MAC address must be in the format H-H-H.

slot *slot-number*: Displays the IPv6 source guard entries on an IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 source binding** to display IPv6 source guard entries.

Note the following when you do not use the **static** keyword:

- If you do not specify any other parameters either, the command displays static and dynamic IPv6 binding entries on all ports and the global static IPv6 binding entries on the master device.

Note the following when you use the **static** keyword: If you do not specify any other parameters, the command displays all global and port-based static IPv6 binding entries.

Related commands: **ipv6 verify source** and **ipv6 source binding**.

Examples

# Display all IPv6 source guard entries.

```
<Sysname> display ipv6 source binding
Total entries found: 4
 MAC Address          IP Address         VLAN      Interface      Type
 040a-0000-0013       2001::4            N/A       N/A            Static-IPv6
 040a-0000-0001       2001::1            N/A       GE1/0/1        Static-IPv6
 040a-0000-0001       2001::3            2         GE1/0/1        DHCPv6-SNP
 040a-0000-0002       2001::4            6         GE1/0/2        ND-SNP
```

# Display all static IPv6 source guard entries.

```
<Sysname> display ipv6 source binding static
Total entries found: 3
 MAC Address          IP Address         VLAN      Interface      Type
 040a-0000-0011       2001::3            N/A       N/A            Static-IPv6
 040a-0000-0012       2001::4            N/A       GE1/0/3        Static-IPv6
 040a-0000-0013       2001::5            N/A       GE1/0/3        Static-IPv6
```

Table 41 Command output

Field	Description
Total entries found	Total number of found entries
MAC Address	MAC address bound in the entry. N/A means that no MAC address is bound in the entry.

Field	Description
IPv6 Address	IPv6 address bound in the entry. N/A means that no IP address is bound in the entry.
VLAN	VLAN bound in the entry. N/A means that no VLAN information exists in the entry.
Interface	Interface of the binding entry. N/A means that the entry is a global static binding entry.
Type	Type of the IPv6 source guard entry: • **Static-IPv6**—Static IPv6 binding entry • **DHCPv6-SNP**—Entry generated based on DHCPv6 snooping entry • **ND-SNP**—Entry generated based on ND snooping entry

ip source binding (interface view)

Syntax

ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding entry. The IPv4 address cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

vlan *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range of 1 to 4094.

Description

Use **ip source binding** to configure a static IPv4 source guard entry on a port.

Use **undo ip source binding** to delete a static IPv4 source guard entry from a port.

By default, no static IPv4 binding entry exists on a port.

IP source guard does not use the VLAN information (if specified) in static IPv4 binding entries to filter packets.

When the ARP detection function is configured, be sure to specify the VLAN where ARP detection is configured in static IPv4 binding entries. Otherwise, ARP packets are discarded because they cannot match any static IPv4 binding entry. For more information about the ARP detection function, see *Security Configuration Guide*.

You cannot configure the same static binding entry repeatedly on one port, but you can configure the same static entry on different ports.

You cannot configure a static binding entry on a port that is in an aggregation group.

Related commands: **display ip source binding static**.

Examples

# Configure a static IPv4 binding entry (IP+MAC binding) on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

ip source binding (system view)

Syntax

ip source binding ip-address *ip-address* **mac-address** *mac-address*

undo ip source binding { **all** | **ip-address** *ip-address* **mac-address** *mac-address* }

View

System view

Default level

2: System level

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding entry. The IPv4 address cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

all: Specifies all global static binding entries.

Description

Use **ip source binding** in system view to configure a global static IPv4 source guard entry.

Use **undo ip source binding** in system view to delete one or all global static IPv4 source guard entries.

By default, no global static IPv4 binding entry exists.

A global static IPv4 binding entry takes effect on all ports.

Related commands: **display ip source binding static**.

Examples

# Configure a global static IPv4 binding entry to bind IP address 192.168.0.1 with MAC address 0001-0001-0001.

```
<Sysname> system-view
[Sysname] ip source binding ip-address 192.168.0.1 mac-address 0001-0001-0001
```

ip verify source

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

View

Layer 2 Ethernet interface view, VLAN interface view, port group view

Default level

2: System level

Parameters

ip-address: Binds source IPv4 addresses to the port.

ip-address mac-address: Binds source IPv4 addresses and MAC addresses to the port.

mac-address: Binds source MAC addresses to the port.

Description

Use **ip verify source** to enable the IPv4 source guard function on a port and specify the elements to be included in the port's dynamic binding entries.

Use **undo ip verify source** to restore the default.

By default, the IPv4 source guard function is disabled on a port.

After you configure the IPv4 source guard function on a port, IPv4 source guard dynamically generates IPv4 source guard entries based on the DHCP snooping entries (on a Layer 2 Ethernet port) or the DHCP-relay entries (on a VLAN interface), and all static IPv4 source guard entries on the port become effective.

You cannot configure the IPv4 source guard function on a port that is in an aggregation group.

Related commands: **display ip source binding**.

Examples

# Configure dynamic IPv4 binding on Layer 2 Ethernet port GigabitEthernet 1/0/1 to filter packets based on the source IPv4 address and MAC address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

# Configure dynamic IPv4 binding on VLAN-interface 100 to filter packets based on the source IPv4 address and MAC address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip verify source ip-address mac-address
```

ip verify source max-entries

Syntax

ip verify source max-entries *number*

undo ip verify source max-entries

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

number: Maximum number of IPv4 source guard entries allowed on a port. The value is in the range of 0 to 640.

Description

Use **ip verify source max-entries** to set the maximum number of static and dynamic IPv4 source guard entries on a port. When the number of IPv4 binding entries on a port reaches the maximum, the port does not allowed new IPv4 binding entries any more.

Use **undo ip verify source max-entries** to restore the default.

By default, the maximum number of IPv4 source guard entries allowed on a port is 640.

If the maximum number of IPv4 binding entries to be configured is smaller than the number of existing IPv4 binding entries on the port, the maximum number can be configured successfully and the existing entries are not affected. New IPv4 binding entries, however, cannot be added any more unless the number of IPv4 binding entries on the port drops below the configured maximum.

Examples

# Set the maximum number of IPv4 source guard entries to 100 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source max-entries 100
```

ipv6 source binding (interface view)

Syntax

ipv6 source binding { **ipv6-address** *ipv6-address* | **ipv6-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **ipv6-address** *ipv6-address* | **ipv6-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding entry. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range of 1 to 4094.

Description

Use **ipv6 source binding** to configure a static IPv6 source guard entry on a port.

Use **undo ipv6 source binding** to delete a static IPv6 source guard entry from a port.

By default, no static IPv6 binding entry exists on a port.

IP source guard does not use the VLAN information (if specified) in static IPv6 binding entries to filter packets.

When the ND detection function is configured, be sure to specify the VLAN where ND detection is configured in static IPv6 binding entries. Otherwise, ND packets are discarded because they cannot match any static IPv6 binding entry. For more information about the ND detection function, see *Security Configuration Guide*.

You cannot configure the same static binding entry repeatedly on one port, but you can configure the same static entry on different ports.

You cannot configure a static binding entry on a port that is in an aggregation group.

Related commands: **display ipv6 source binding static**.

Examples

# Configure a static IPv6 binding entry (IP+MAC binding) on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 source binding ipv6-address 2001::1 mac-address
0002-0002-0002
```

ipv6 source binding (system view)

Syntax

ipv6 source binding ipv6-address *ipv6-address* **mac-address** *mac-address*

undo ipv6 source binding { **all** | **ipv6-address** *ipv6-address* **mac-address** *mac-address* }

View

System view

Default level

2: System level

Parameters

Ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding entry. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Specifies all global static binding entries.

Description

Use **ipv6 source binding** in system view to configure a global static IPv6 source guard entry.

Use **undo ipv6 source binding** in system view to delete one or all global static IPv6 source guard entries.

By default, no global static IPv6 binding entry exists.

A global static IPv6 binding entry takes effect on all ports.

Related commands: **display ipv6 source binding static**.

Examples

# Configure a global static IPv6 binding entry to bind IP address 2001::1 with MAC address 0002-0002-0002.

```
<Sysname> system-view
[Sysname] ipv6 source binding ipv6-address 2001::1 mac-address 0002-0002-0002
```

ipv6 verify source

Syntax

ipv6 verify source { **ipv6-address** | **ipv6-address mac-address** | **mac-address** }

undo ipv6 verify source

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

ipv6-address: Binds source IPv6 addresses to the port.

ipv6-address mac-address: Binds source IPv6 addresses and MAC addresses to the port.

mac-address: Binds source MAC addresses to the port.

Description

Use **ipv6 verify source** to enable the IPv6 source guard function on a port and specify the elements to be included in the port's dynamic binding entries.

Use **undo ipv6 verify source** to restore the default.

By default, the IPv6 source guard function is disabled on a port.

After you configure the IPv6 source guard function on a port, the IPv6 source guard function dynamically generates IPv6 source guard entries based on the DHCPv6 snooping entries or ND snooping entries, and all static IPv6 source guard entries become effective.

You cannot configure the IPv6 source guard function on a port that is in an aggregation group.

Related commands: **display ipv6 source binding**.

Examples

# Configure dynamic IPv6 binding on Layer 2 Ethernet port GigabitEthernet 1/0/1 to filter IPv6 packets based on the source IPv6 address and MAC address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

ipv6 verify source max-entries

Syntax

ipv6 verify source max-entries *number*

undo ipv6 verify source max-entries

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

number: Maximum number of IPv6 source guard entries allowed on a port. The value is in the range of 0 to 640.

Description

Use **ipv6 verify source max-entries** to set the maximum number of static and dynamic IPv6 source guard entries on a port. When the number of IPv6 binding entries on a port reaches the maximum, the port does not allowed new IPv6 binding entries any more.

Use **undo ipv6 verify source max-entries** to restore the default.

By default, the maximum number of IPv6 source guard entries allowed on a port is 640.

If the maximum number of IPv6 binding entries to be configured is smaller than the number of existing IPv6 binding entries on the port, the maximum number can be configured successfully and the existing entries are not affected. New IPv6 binding entries, however, cannot be added any more unless the number of IPv6 binding entries on the port drops below the configured maximum.

Examples

# Set the maximum number of IPv6 source guard entries to 100 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 verify source max-entries 100
```

ARP attack protection configuration commands

ARP defense against IP packet attacks configuration commands

arp resolving-route enable

Syntax

arp resolving-route enable

undo arp resolving-route enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp resolving-route enable** to enable ARP black hole routing.

Use **undo arp resolving-route enable** to disable the function.

By default, the function is enabled.

Examples

# Enable ARP black hole routing.

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

arp source-suppression enable

Syntax

arp source-suppression enable

undo arp source-suppression enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp source-suppression enable** to enable the ARP source suppression function.

Use **undo arp source-suppression enable** to disable the function.

By default, the ARP source suppression function is disabled.

Related commands: **display arp source-suppression**.

Examples

# Enable the ARP source suppression function.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

View

System view

Default level

2: System level

Parameters

limit-value: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds. It ranges from 2 to 1024.

Description

Use **arp source-suppression limit** to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds.

Use **undo arp source-suppression limit** to restore the default value, which is 10.

With this feature configured, whenever the number of packets with unresolvable destination IP addresses from a host within five seconds exceeds the specified threshold, the device suppresses the sending host from triggering any ARP requests within the following five seconds.

Related commands: **display arp source-suppression**.

Examples

# Set the maximum number of packets with the same source address but unresolvable destination IP addresses that the device can receive in five seconds to 100.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax

display arp source-suppression [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Examples

# Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
 Current cache length: 16
```

Table 42 Command output

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled.
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds.
Current cache length	Size of cache used to record source suppression information.

ARP packet rate limit configuration commands

arp rate-limit

Syntax

arp rate-limit { **disable** | **rate** *pps* **drop** }

undo arp rate-limit

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

disable: Disables ARP packet rate limit.

rate *pps*: Specifies the ARP packet rate in pps, in the range of 5 to 100.

drop: Discards the exceeded packets.

Description

Use **arp rate-limit** to configure or disable ARP packet rate limit on an interface.

Use **undo arp rate-limit** to restore the default.

By default, ARP packet rate limit is disabled.

Examples

# Specify the ARP packet rate on layer 2 Ethernet port GigabitEthernet 1/0/1 as 50 pps, and exceeded packets will be discarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit rate 50 drop
```

arp rate-limit information

Syntax

arp rate-limit information interval *seconds*

undo arp rate-limit information

View

System view

Default level

2: System level

Parameters

interval *seconds*: Specifies the interval for sending trap and log messages when ARP packet rate exceeds the threshold rate. The *seconds* argument ranges from 1 to 86400, in seconds.

Description

Use **arp rate-limit information** to set the interval for sending trap and log messages when ARP packet rate exceeds the threshold rate.

Use **undo arp rate-limit information** to restore the default.

By default, the interval is 60 seconds.

This command must work in cooperation with the **arp rate-limit** command.

Examples

# Configure the device to send trap and log messages every 120 seconds when ARP packet rate exceeds the threshold rate.

```
<Sysname> system-view
[Sysname] arp rate-limit information interval 120
```

Source MAC address based ARP attack detection configuration commands

arp anti-attack source-mac

Syntax

arp anti-attack source-mac { **filter** | **monitor** }

undo arp anti-attack source-mac [**filter** | **monitor**]

View

System view

Default level

2: System level

Parameters

filter: Specifies the **filter** mode.

monitor: Specifies the **monitor** mode.

Description

Use **arp anti-attack source-mac** to enable source MAC address based ARP attack detection and specify the detection mode.

Use **undo arp anti-attack source-mac** to restore the default.

By default, source MAC address based ARP attack detection is disabled.

After you enable this feature, the device checks the source MAC address of ARP packets received from the VLAN. It detects an attack when one MAC address sends more ARP packets in five seconds than the specified threshold. Upon detecting an attack, the device does the following:

- In filter detection mode, the device generates a log message and filters out the ARP packets from the MAC address.
- In monitor detection mode, the device only generates a log message.

If no detection mode is specified in the **undo arp anti-attack source-mac** command, both detection modes are disabled.

Examples

# Enable filter-mode source MAC address based ARP attack detection

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac filter
```

arp anti-attack source-mac aging-time

Syntax

arp anti-attack source-mac aging-time *time*

undo arp anti-attack source-mac aging-time

View

System view

Default level

2: System level

Parameters

time: Specifies the age timer for protected MAC addresses, in the range of 60 to 6000 seconds.

Description

Use **arp anti-attack source-mac aging-time** to configure the age timer for protected MAC addresses.

Use **undo arp anti-attack source-mac aging-time** to restore the default.

By default, the age timer for protected MAC addresses is 300 seconds (five minutes).

Examples

# Configure the age timer for protected MAC addresses as 60 seconds.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

arp anti-attack source-mac exclude-mac

Syntax

arp anti-attack source-mac exclude-mac *mac-address*&<1-10>

undo arp anti-attack source-mac exclude-mac [*mac-address*&<1-10>]

View

System view

Default level

2: System level

Parameters

mac-address&<1-10>: Specifies a MAC address list. The *mac-address* argument indicates a protected MAC address in the format H-H-H. &<1-10> indicates the number of protected MAC addresses that you can configure.

Description

Use **arp anti-attack source-mac exclude-mac** to configure protected MAC addresses that are excluded from ARP packet detection.

Use **undo arp anti-attack source-mac exclude-mac** to remove the configured protected MAC addresses.

By default, no protected MAC address is configured.

If no MAC address is specified in the **undo arp anti-attack source-mac exclude-mac** command, all the configured protected MAC addresses are removed.

Examples

# Configure a protected MAC address.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

arp anti-attack source-mac threshold

Syntax

arp anti-attack source-mac threshold *threshold-value*

undo arp anti-attack source-mac threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Specifies the threshold for source MAC address based ARP attack detection, in the range of 10 to 100.

Description

Use **arp anti-attack source-mac threshold** to configure the threshold for source MAC address based ARP attack detection. If the number of ARP packets sent from a MAC address within five seconds exceeds this threshold, the device considers this an attack.

Use **undo arp anti-attack source-mac threshold** to restore the default.

By default, the threshold for source MAC address based ARP attack detection is 50.

Examples

# Configure the threshold for source MAC address based ARP attack detection as 30.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac threshold 30
```

display arp anti-attack source-mac

Syntax

display arp anti-attack source-mac { **slot** *slot-number* | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays attacking MAC addresses detected on the interface.

slot *slot-number*: Displays attacking MAC addresses detected on a specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp anti-attack source-mac** to display attacking MAC addresses detected by source MAC address based ARP attack detection.

If no interface is specified, the **display arp anti-attack source-mac** command displays attacking MAC addresses detected on all the interfaces.

Examples

# Display the attacking MAC addresses detected by source MAC address based ARP attack detection.

```
<Sysname> display arp anti-attack source-mac slot 1
Source-MAC          VLAN ID            Interface             Aging-time
23f3-1122-3344      4094               GE1/0/1               10
23f3-1122-3355      4094               GE1/0/2               30
23f3-1122-33ff      4094               GE1/0/3               25
23f3-1122-33ad      4094               GE1/0/4               30
23f3-1122-33ce      4094               GE1/0/5               2
```

ARP packet source mac address consistency check configuration commands

arp anti-attack valid-check enable

Syntax

arp anti-attack valid-check enable

undo arp anti-attack valid-check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp anti-attack valid-check enable** to enable ARP packet source MAC address consistency check on the gateway. After you execute this command, the gateway device can filter out ARP packets with the source MAC address in the Ethernet header different from the sender MAC address in the ARP message.

Use **undo arp anti-attack valid-check enable** to restore the default.

By default, ARP packet source MAC address consistency check is disabled.

Examples

# Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

ARP active acknowledgement configuration commands

arp anti-attack active-ack enable

Syntax

arp anti-attack active-ack enable

undo arp anti-attack active-ack enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp anti-attack active-ack enable** to enable the ARP active acknowledgement function.

Use **undo arp anti-attack active-ack enable** to restore the default.

By default, the ARP active acknowledgement function is disabled.

This feature is configured on gateway devices to identify invalid ARP packets.

Examples

# Enable the ARP active acknowledgement function.

```
<Sysname> system-view
[Sysname] arp anti-attack active-ack enable
```

ARP detection configuration commands

arp detection

Syntax

arp detection *id-number* { **permit** | **deny** } **ip** { **any** | *ip-address* [*ip-address-mask*] } **mac** { **any** | *mac-address* [*mac-address-mask*] } [**vlan** *vlan-id*]

undo arp detection *id-number*

Views

System view

Default level

2: System level

Parameters

id-number: Specifies the ID of the rule, in the range of 0 to 511. A lower value refers to a higher priority.

deny: Denies ARP packets matching the rule.

permit: Permit ARP packets matching the rule.

ip { **any** | *ip-address* [*ip-address-mask*] }: Specifies an IP address range for matching sender IP addresses of ARP packets.

- **any**: Matches any sender IP address.
- *ip*-address: Matches the specified sender IP address.
- ip-*address-mask*: Specifies a mask for the IP address, in dotted-decimal format. The *ip-address* argument without a mask indicates a host address.

mac { **any** | *mac-address* [*mac-address-mask*] }: Specifies a MAC address range for matching sender MAC addresses of ARP packets.

- **any**: Matches any sender MAC address.
- mac-address: Matches the specified sender MAC address, in the format of H-H-H.
- m*ac-address-mask:* Specifies a mask for the MAC address, in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN where the rule applies. The *vlan-id* argument is in the range of 1 to 4094.

Description

Use **arp detection** to set a rule for user validity check.

Use **undo arp detection** to restore the default.

By default, no rule is set for user validity check.

User validity check inspects each ARP packet received on an ARP untrusted interface against the configured rules. If a match is found, the ARP packet is processed according to the matching rule; if no match is found, the device checks the packet against static IP Source Guard binding entries, the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses in turn.

Related command: **arp detection enable**.

Examples

# Set a rule for user validity check and enable user validity check.

```
<Sysname> system-view
[Sysname] arp detection 0 permit ip 3.1.1.1 255.255.0.0 mac 0001-0203-0607 ffff-ffff-0000
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

arp detection enable

Syntax

arp detection enable

undo arp detection enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **arp detection enable** to enable ARP detection for the VLAN.

Use **undo arp detection enable** to restore the default.

By default, ARP detection is disabled for a VLAN.

Examples

# Enable ARP detection for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

arp detection trust

Syntax

arp detection trust

undo arp detection trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **arp detection trust** to configure the port as an ARP trusted port.

Use **undo arp detection trust** to restore the default.

By default, the port is an ARP untrusted port.

Examples

# Configure layer 2 Ethernet port GigabitEthernet 1/0/1 as an ARP trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

View

System view

Default level

2: System level

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this keyword specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests will be checked.

src-mac: Checks whether the sender MAC address of an ARP packet is identical to the source MAC address in the Ethernet header. If they are identical, the packet is considered valid; otherwise, the packet is discarded.

Description

Use **arp detection validate** to configure ARP detection based on specified objects. You can specify one or more objects in one command line.

Use **undo arp detection validate** to remove detected objects. If no keyword is specified, all the detected objects are removed.

By default, ARP detection based on specified objects is disabled.

Examples

# Enable the checking of the MAC addresses and IP addresses of ARP packets.

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac src-mac ip
```

arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

By default, ARP restricted forwarding is disabled.

Examples

# Enable ARP restricted forwarding in VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp restricted-forwarding enable
```

display arp detection

Syntax

display arp detection [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp detection** to display the VLAN(s) enabled with ARP detection.

Related commands: **arp detection enable**.

Examples

# Display the VLANs enabled with ARP detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1, 2, 4-5
```

Table 43 Command output

Field	Description
ARP detection is enabled in the following VLANs	VLANs that are enabled with ARP detection

display arp detection statistics

Syntax

display arp detection statistics [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the ARP detection statistics of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp detection statistics** to display statistics about ARP detection. This command only displays numbers of discarded packets. If no interface is specified, the statistics of all the interfaces will be displayed.

Examples

# Display the ARP detection statistics of all the interfaces.

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP         Src-MAC    Dst-MAC    Inspect
GE1/0/1(U)                 40         0          0          78
GE1/0/2(U)                 0          0          0          0
GE1/0/3(T)                 0          0          0          0
GE1/0/4(U)                 0          0          30         0
```

Table 44 Command output

Field	Description
Interface(State)	State T or U identifies a trusted or untrusted port.
IP	Number of ARP packets discarded due to invalid source and destination IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass ARP detection (based on static IP Source Guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses).

reset arp detection statistics

Syntax

reset arp detection statistics [**interface** *interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears the ARP detection statistics of a specified interface.

Description

Use **reset arp detection statistics** to clear ARP detection statistics of a specified interface. If no interface is specified, the statistics of all the interfaces will be cleared.

Examples

# Clear the ARP detection statistics of all the interfaces.

```
<Sysname> reset arp detection statistics
```

ARP automatic scanning and fixed ARP configuration commands

arp fixup

Syntax

arp fixup

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp fixup** to change the existing dynamic ARP entries into static ARP entries. You can use this command again to change the dynamic ARP entries learned later into static ARP entries.

The static ARP entries changed from dynamic ARP entries have the same attributes as the manually configured static ARP entries.

The number of static ARP entries changed from dynamic ARP entries is restricted by the number of static ARP entries that the device supports. As a result, the device may fail to change all dynamic ARP entries into static ARP entries.

Suppose that the number of dynamic ARP entries is *D* and that of the existing static ARP entries is *S*. When the dynamic ARP entries are changed into static, new dynamic ARP entries may be created (suppose the number is *M*) and some of the dynamic ARP entries may be aged out (suppose the number is *N*). After the process is complete, the number of static ARP entries is *D* + *S* + *M* – *N*.

To delete a specific static ARP entry changed from a dynamic one, use the **undo arp** *ip-address* command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

# Enable fixed ARP.

```
<Sysname> system-view
[Sysname] arp fixup
```

arp scan

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*]

View

VLAN interface view

Default level

2: System level

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

Description

Use **arp scan** to enable ARP automatic scanning in the specified address range for neighbors.

If the start IP and end IP addresses are specified, the device scans the specific address range for neighbors and learns their ARP entries, so that the scanning time is reduced. If the specified address range contains multiple network segments, the sender IP address in the ARP request is the interface address on the smallest network segment.

If no address range is specified, the device only scans the network where the primary IP address of the interface resides for neighbors. The sender IP address in the ARP requests is the primary IP address of the interface.

The start IP address and end IP address must be on the same network as the primary IP address or manually configured secondary IP addresses of the interface.

IP addresses that already exist in ARP entries are not scanned.

ARP automatic scanning may take some time. To stop an ongoing scan, press **Ctrl** + **C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

Examples

# Configure the device to scan the network where the primary IP address of VLAN-interface 2 resides for neighbors.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

# Configure the device to scan a specific address range for neighbors.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

ARP gateway protection configuration commands

arp filter source

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a protected gateway.

Description

Use **arp filter source** to enable ARP gateway protection for a specified gateway.

Use **undo arp filter source** to disable ARP gateway protection for a specified gateway.

By default, ARP gateway protection is disabled.

You can enable ARP gateway protection for up to eight gateways on a port.

You cannot configure both the **arp filter source** and **arp filter binding** commands on a port.

Examples

# Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

ARP filtering configuration commands

arp filter binding

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ip-address: Specifies the permitted sender IP address.

mac-address: Specifies the permitted sender MAC address.

Description

Use **arp filter binding** to configure an ARP filtering entry. If the sender IP and MAC addresses of an ARP packet match an ARP filtering entry, the ARP packet is permitted. If not, it is discarded.

Use **undo arp filter binding** to remove an ARP filtering entry.

By default, no ARP filtering entry is configured.

You can configure up to eight ARP filtering entries on a port.

You cannot configure both the **arp filter source** and **arp filter binding** commands on a port.

Examples

# Configure an ARP filtering entry with permitted sender IP address 1.1.1.1 and MAC address 2-2-2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 2-2-2
```

ND attack defense configuration commands

Source MAC consistency check commands

ipv6 nd mac-check enable

Syntax

ipv6 nd mac-check enable

undo ipv6 nd mac-check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd mac-check enable** to enable source MAC consistency check for ND packets.

Use **undo ipv6 nd mac-check enable** to disable source MAC consistency check for ND packets.

By default, source MAC consistency check is disabled for ND packets.

In a typical forged ND packet, the Ethernet frame header conveys a source MAC address different than the source link layer address option. To filter out these invalid ND packets, use the source MAC consistency check function to check ND packets for MAC address inconsistency.

Examples

# Enable source MAC consistency check for ND packets.

```
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

ND detection configuration commands

display ipv6 nd detection

Syntax

display ipv6 nd detection [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, seethe *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd detection** to display ND detection configuration.

Related commands: **ipv6 nd detection enable** and **ipv6 nd detection trust**.

Examples

# Display ND detection configuration.

```
<Sysname> display ipv6 nd detection
ND detection is enabled on the following VLANs:
 1, 2, 4-5
ND detection trust is configured on the following interfaces:
 GigabitEthernet1/0/1
 GigabitEthernet1/0/2
```

Table 45 Command output

Field	Description
ND detection is enabled on the following VLANs	List of VLANs enabled with ND detection.
ND detection trust is configured on the following interfaces	List of ND-trusted ports. On an ND-trusted port, ND packets are not checked. By default, all ports are ND-untrusted ports on which ND packets in an ND detection-enabled VLAN will be checked.

display ipv6 nd detection statistics

Syntax

display ipv6 nd detection statistics [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays ND detection statistics for the interface identified by *interface-type interface-number*. The *interface-type interface-number* arguments represent the interface type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd detection statistics** to display ND detection statistics. The statistics count only ND packets discarded for validity check failure.

If an interface is specified, the command displays only the statistic for the interface. If no interface is specified, the command displays statistics for all interfaces.

Examples

# Display the statistics for discarded ND packets on all interfaces.

```
<Sysname> display ipv6 nd detection statistics
ND packets dropped by ND detection:
Interface         Packets Dropped
GE1/0/1             78
GE1/0/2             0
GE1/0/3             0
GE1/0/4             0
```

ipv6 nd detection enable

Syntax

ipv6 nd detection enable

undo ipv6 nd detection enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd detection enable** to enable ND detection in a VLAN to check ND packets for source spoofing.

Use **undo ipv6 nd detection enable** to disable ND detection.

By default, ND detection is disabled.

Examples

# Enable ND detection in VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan 10] ipv6 nd detection enable
```

ipv6 nd detection trust

Syntax

ipv6 nd detection trust

undo ipv6 nd detection trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd detection trust** to configure a port as an ND-trusted port.

Use **undo ipv6 nd detection trust** to configure a port as an ND-untrusted port.

By default, a port is ND-untrusted. In an ND detection-enabled VLAN, ports are assigned two roles: ND-trusted and ND-untrusted.

On an ND-trusted port, the ND detection function does not check ND packets for address spoofing.

On an ND-untrusted port, RA and RR messages are considered illegal and discarded directly; all other ND packets in the VLAN are checked for source spoofing.

Examples

# Configure Layer 2 port GigabitEthernet1/0/1 as an ND-trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname- GigabitEthernet1/0/1] ipv6 nd detection trust
```

# Configure interface Bridge-Aggregation 1 as an ND-trusted port.

```
<Sysname> system-view
[Sysname] interface bridge-Aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd detection trust
```

reset ipv6 nd detection statistics

Syntax

reset ipv6 nd detection statistics [**interface** *interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears the statistics of the interface identified by *interface-type interface-number*. The *interface-type interface-number* arguments represent the interface type and number.

Description

Use **reset ipv6 nd detection statistics** to clear the ND detection statistics of an interface. If no interface is specified, the ND detection statistics of all interfaces are cleared.

Examples

# Clear the ND detection statistics of all interfaces.

```
<Sysname> reset ipv6 nd detection statistics
```

SAVI configuration commands

ipv6 savi dad-delay

Syntax

ipv6 savi dad-delay *value*

undo ipv6 savi dad-delay

View

System view

Default level

2: System level

Parameters

value: Specifies the time in centiseconds to wait for a duplicate address detection (DAD) NA, ranging from 0 to 2147483647.

Description

Use **ipv6 savi dad-delay** to set the time to wait for a DAD NA.

Use **undo ipv6 savi dad-delay** to restore the default.

By default, the time to wait for a DAD NA is 100 centiseconds (1 second).

Examples

# Set the time to wait for a DAD NA to 100 seconds.

```
<Sysname> system-view
[Sysname] ipv6 savi dad-delay 10000
```

ipv6 savi dad-preparedelay

Syntax

ipv6 savi dad-preparedelay *value*

undo ipv6 savi dad-preparedelay

View

System view

Default level

2: System level

Parameters

value: Specifies the time in centiseconds to wait for a DAD NS from a DHCPv6 client after the DHCPv6 client obtains an IP address. This argument ranges from 0 to 2147483647.

Description

Use **ipv6 savi dad-preparedelay** to set the time to wait for a DAD NS from a DHCPv6 client.

Use **undo ipv6 savi dad-preparedelay** to restore the default.

By default, the time to wait for a DAD NS from a DHCPv6 client is 100 centiseconds (1 second).

This command is used with the DHCPv6 snooping function. After DHCPv6 snooping detects that a client obtains an IPv6 address, it monitors whether the client detects IP address conflict. If DHCPv6 snooping does not receive any DAD NS from the client before the set time expires, SAVI sends a DAD NS on behalf of the client.

Examples

# Set the time to wait for a DAD NS from a DHCPv6 client to 100 seconds.

```
<Sysname> system-view
[Sysname] ipv6 savi dad-preparedelay 10000
```

ipv6 savi strict

Syntax

ipv6 savi strict

undo ipv6 savi strict

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 savi strict** to enable the SAVI function.

Use **undo ipv6 savi strict** to disable the SAVI function.

By default, the SAVI function is disabled.

NOTE:

If a port on the SAVI enabled device is down for three minutes or more, the device deletes the DHCPv6 snooping entries and ND snooping entries corresponding to the port.

Examples

# Enable the SAVI function.

```
<Sysname> system-view
[Sysname] ipv6 savi strict
```

Blacklist configuration commands

blacklist enable

Syntax

blacklist enable

undo blacklist enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **blacklist enable** to enable the blacklist feature. With the blacklist feature enabled, the switch filters all packets from IP addresses on the blacklist.

Use **undo blacklist enable** to restore the default.

By default, the blacklist feature is disabled.

After you enable the blacklist feature, you can manually add blacklist entries, or have the switch cooperate with the login user authentication feature to add blacklist entries automatically.

Examples

# Enable the blacklist feature.

```
<Sysname> system-view
[Sysname] blacklist enable
```

blacklist ip

Syntax

blacklist ip *source-ip-address* [**timeout** *minutes*]

undo blacklist { **all** | **ip** *source-ip-address* [**timeout**] }

View

System view

Default level

2: System level

Parameters

source-ip-address: IP address to be added to the blacklist. It cannot be the broadcast address, 127.0.0.0/8, a class D address, or a class E address.

all: Specifies all blacklist entries.

timeout *minutes*: Specifies the aging time for the entry in minutes, in the range of 1 to 1000. If you do not specify this option, the entry does not age and is always effective, unless you manually remove it.

Description

Use **blacklist ip** to add a blacklist entry. Then, the blacklist feature filters all packets from the IP address before the entry is aged out or manually removed.

Use **undo blacklist** to remove all blacklist entries in one operation, remove a single blacklist entry, or cancel the aging time setting of a blacklist entry.

The **undo blacklist ip** *source-ip-address* **timeout** command does not remove the entry; it only cancels the aging time setting of the entry, making the entry never aging out.

Blacklist entries are effective only when the blacklist feature is enabled.

You can change the aging time of an existing blacklist entry, and your change takes effect immediately.

Related commands: **blacklist enable** and **display blacklist**.

Examples

# Add the IP address 192.168.1.2 to the blacklist, and set the aging time to 20 minutes.

```
<Sysname> system-view
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

display blacklist

Syntax

display blacklist { **all** | **ip** *source-ip-address* [**slot** *slot-number*] | **slot** *slot-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip *source-ip-address*: Displays information about the blacklist entry for an IP address. The *source-ip-address* argument cannot be the broadcast address, 127.0.0.0/8, a class D address, or a class E address.

all: Displays information about all blacklist entries.

slot *slot-number*: Displays information about the blacklist entries on an IRF member device. The *slot-number* argument represents the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display blacklist** to display blacklist information.

Related commands: **blacklist enable** and **blacklist ip**.

Examples

# Display information about all blacklist entries.

```
<Sysname> display blacklist all
                    Blacklist information
------------------------------------------------------------------------------
Blacklist                             : enabled
Blacklist items                       : 1
------------------------------------------------------------------------------
IP              Type   Aging started       Aging finished      Dropped packets
                       YYYY/MM/DD hh:mm:ss YYYY/MM/DD hh:mm:ss
2.2.1.2         manual 2011/05/27 19:15:39 Never               0
1.1.1.2         auto   2011/05/01 18:26:31 2011/05/01 18:36:31 4294967295
1.1.1.3         manual 2011/05/02 06:13:20 2011/05/02 07:54:47 4294967295
--------------------------------------------------------------------------
```

Table 46 Command output

Field	Description
Blacklist	Whether the blacklist feature is enabled.
Blacklist items	Number of blacklist entries.
IP	IP address of the blacklist entry.
Type	Type of the blacklist entry: • **manual**—The entry was manually added. • **auto**—The entry was automatically added.
Aging started	Installation time of the entry.
Aging finished	Expiration time of the entry. For an entry with no aging time setting, the value Never is displayed.
Dropped packets	Number of packets from the IP address that have been dropped.

Index

Contents

Ethernet OAM configuration commands

display oam

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

local: Displays local Ethernet OAM connection information.

remote: Displays remote Ethernet OAM connection information.

interface *interface-type interface-number*: Specifies a port by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display oam** to display information about an Ethernet OAM connection, including connection status, information contained in the Ethernet OAM packet header, and Ethernet OAM packet statistics.

If no interface is specified, this command displays information about all Ethernet OAM connections.

Related commands: **reset oam**.

Examples

# Display information about the Ethernet OAM connection established on the local port GigabitEthernet 1/0/1.

```
<Sysname> display oam local interface gigabitethernet 1/0/1
Port        : GigabitEthernet1/0/1
Link Status : Up
EnableStatus                : Enable
Local_oam_mode              : Active      Local_pdu               : ANY
Local_mux_action            : FWD         Local_par_action        : FWD

OAMLocalFlagsField :
---------------------------------------------------------------------------
Link Fault                  : 0           Dying Gasp              : 0
```

```
Critical Event              : 0           Local Evaluating       : COMPLETE
Remote Evaluating           : COMPLETE

Packets statistic :
Packets                        Send                    Receive
--------------------------------------------------------------------------
OAMPDU                         645                     648
OAMInformation                 645                     648
OAMEventNotification           0                       --
OAMUniqueEventNotification     --                      0
OAMDuplicateEventNotification  --                      0
```

Table 1 Command output

Field	Description
Port	Port index.
Link Status	Link status (up or down).
EnableStatus	Ethernet OAM state (enabled or disabled).
Local_oam_mode	Local Ethernet OAM mode, which can be: • **Active**—The port is operating in active Ethernet OAM mode. • **Passive**—The port is operating in passive Ethernet OAM mode.
Local_pdu	The way in which the local end processes Ethernet OAMPDUs: • **RX_INFO**—The port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. • **LF_INFO**—The port only sends the Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • **INFO**—The port sends and receives only Information OAMPDUs. • **ANY**—The port sends and receives Ethernet OAMPDUs of any type.
Local_mux_action	Working mode of the local transmitter: • **FWD**—The port can send any packets. • **DISCARD**—The port only sends Ethernet OAMPDUs.
Local_par_action	Working mode of the local receiver: • **FWD**—The port can receive any packets. • **DISCARD**—The port only receives Ethernet OAMPDUs. • **LB**—The local receiver is in loopback state. All the packets other than Ethernet OAMPDUs received on the local receiver are returned to their sources along the ways they came.
OAMLocalFlagsField	Local flags inserted in the local flag fields of the Ethernet OAMPDUs sent.
Link Fault	Indicates whether an Ethernet OAM link error is present: 0 for no and 1 for yes.
Dying Gasp	Indicates whether a fatal error is present: 0 for no and 1 for yes.
Critical Event	Indicates whether a critical error is present: 0 for no and 1 for yes.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • COMPLETE for completed. • Others for uncompleted.

Field	Description
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: - COMPLETE for completed. - Others for uncompleted.
Packets statistic	Statistics for Ethernet OAMPDUs sent and received.
OAMPDU	Total number of the Ethernet OAMPDUs sent and received.
OAMInformation	Number of Information OAMPDUs sent and received.
OAMEventNotification	Number of Event notification OAMPDUs sent and received.
OAMUniqueEventNotification	Number of unduplicated Event notification OAMPDUs sent or received.
OAMDuplicateEventNotification	Number of duplicate Event notification OAMPDUs sent or received.

# Display the Ethernet OAM information for the peer port GigabitEthernet 1/0/1.

```
<Sysname> display oam remote interface gigabitethernet 1/0/1
Port        : GigabitEthernet1/0/1
Link Status : Up
Information of the latest received OAM packet:
OAMRemoteMACAddress       : 00e0-fd73-6502
OAMRemotePDUConfiguration : 1500

OAMRemoteState :
--------------------------------------------------------------------------
Remote_mux_action         : FWD         Remote_par_action      : FWD

OAMRemoteConfiguration :
--------------------------------------------------------------------------
OAM Mode                  : Active      Unidirectional Support : YES
Loopback Support          : NO          Link Events            : YES
Variable Retrieval        : NO

OAMRemoteFlagsField :
--------------------------------------------------------------------------
Link Fault                : 0           Dying Gasp             : 0
Critical Event            : 0           Local Evaluating       : COMPLETE
Remote Evaluating         : COMPLETE
```

Table 2 Command output

Field	Description
Port	Port index.
Link Status	Link status.
Information of the latest received OAM packet	Information about the latest received Ethernet OAMPDU.
OAMRemoteMACAddress	MAC address of the Ethernet OAM peer.

Field	Description
OAMRemotePDUConfiguration	Maximum Ethernet OAMPDU size allowed.
OAMRemoteState	State of the Ethernet OAM peer.
Remote_mux_action	Peer sending mode. For more information, see Table 1.
Remote_par_action	Peer receiving mode. For more information, see Table 1.
OAMRemoteConfiguration	Configuration of the peer Ethernet OAM entity.
OAM Mode	Ethernet OAM mode.
Unidirectional Support	Indicates whether unidirectional transmission is supported (YES or NO).
Loopback Support	Indicates whether Ethernet OAM remote loopback is supported (YES or NO).
Link Events	Indicates whether Ethernet OAM link error events are supported (YES or NO).
Variable Retrieval	Indicates whether MIB variable retrieval is supported (YES or NO).
OAMRemoteFlagsField	Values of the peer Ethernet OAM flag fields in OAM packets.
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes.
Dying Gasp	Indicate whether a fatal fault is present: 0 for no and 1 for yes.
Critical Event	Indicate whether a critical fault is present: 0 for no and 1 for yes.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • COMPLETE for completed. • Others for uncompleted.
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • COMPLETE for completed. • Others for uncompleted.

display oam configuration

Syntax

display oam configuration [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display oam configuration** to display global Ethernet OAM configuration, including the periods and thresholds for Ethernet OAM link error event detection.

Related commands: **oam errored-symbol period**, **oam errored-symbol threshold**, **oam errored-frame period**, **oam errored-frame threshold**, **oam errored-frame-period period**, **oam errored-frame-period threshold**, **oam errored-frame-seconds period**, **oam errored-frame-seconds threshold**, **oam timer hello**, and **oam timer keepalive**.

Examples

# Display global Ethernet OAM configuration.

```
<Sysname> display oam configuration
Configuration of the link event window/threshold :
--------------------------------------------------------------------------
Errored-symbol Event period(in seconds)           :     1
Errored-symbol Event threshold                    :     1
Errored-frame Event period(in seconds)            :     1
Errored-frame Event threshold                     :     1
Errored-frame-period Event period(in ms)          :     1000
Errored-frame-period Event threshold              :     1
Errored-frame-seconds Event period(in seconds)    :     60
Errored-frame-seconds Event threshold             :     1

Configuration of the timer :
--------------------------------------------------------------------------
Hello timer(in ms)                                :     1000
Keepalive timer(in ms)                            :     5000
```

Table 3 Command output

Field	Description
Configuration of the link event window/threshold	Detection intervals and triggering thresholds configured for link events.
Errored-symbol Event period (in seconds)	Errored symbol event detection interval, which defaults to one second.
Errored-symbol Event threshold	Errored symbol event triggering threshold, which defaults to 1.
Errored-frame Event period (in seconds)	Errored frame event detection interval, which defaults to one second.
Errored-frame Event threshold	Errored frame event triggering threshold, which defaults to 1.
Errored-frame-period Event period (in ms)	Errored frame period event detection interval, which defaults to 1000 milliseconds.
Errored-frame-period Event threshold	Errored frame period event triggering threshold, which defaults to 1.
Errored-frame-seconds Event period (in seconds)	Errored frame seconds event detection interval, which defaults to 60 seconds.
Errored-frame-seconds Event threshold	Errored frame seconds event triggering threshold, which defaults to 1.

Field	Description
Configuration of the timer	Ethernet OAM connection detection timers.
Hello timer(in ms)	Ethernet OAM handshake packet transmission interval, the value of which defaults to 1000 milliseconds.
Keepalive timer(in ms)	Ethernet OAM connection timeout timer, the value of which defaults to 5000 milliseconds.

display oam critical-event

Syntax

display oam critical-event [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display oam critical-event** to display the statistics on critical Ethernet OAM link that have events occurred on a port.

If no port is specified, this command displays critical Ethernet OAM link event statistics for all ports.

Examples

# Display critical Ethernet OAM link event statistics for all ports.

```
<Sysname> display oam critical-event
Port        : GigabitEthernet1/0/1
Link Status : Up
Event statistic :
-------------------------------------------------------------------------
Link Fault    :0    Dying Gasp    : 0    Critical Event    : 0
```

Table 4 Command output

Field	Description
Port	Port index

Field	Description
Link Status	Link status
Event statistic	Critical Ethernet OAM link event statistics
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes
Dying Gasp	Indicates whether a fatal fault is present: 0 for no and 1 for yes
Critical Event	Indicates whether a critical fault is present: 0 for no and 1 for yes

display oam link-event

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*] **[|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

local: Displays local Ethernet OAM link error event statistics.

remote: Displays peer Ethernet OAM link error event statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display oam link-event** to display statistics for Ethernet OAM link error events that occurred on a local port or a peer port. Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

If no port is specified, this command displays local or remote Ethernet OAM link error event statistics for all ports.

Related commands: **display oam configuration** and **reset oam**.

Examples

# Display local Ethernet OAM link error event statistics for all ports.

```
<Sysname> display oam link-event local
Port        : GigabitEthernet1/0/1
Link Status : Up
```

```
OAMLocalErrFrameEvent : (ms = milliseconds)
---------------------------------------------------------------------------
Event Time Stamp          : 3539        Errored Frame Window  : 10(100ms)
Errored Frame Threshold   : 5           Errored Frame         : 1488111
Error Running Total       : 260908758   Event Running Total   : 307

OAMLocalErrFramePeriodEvent :
---------------------------------------------------------------------------
Event Time Stamp          : 3539        Errored Frame Window  : 976500
Errored Frame Threshold   : 1           Errored Frame         : 1042054
Error Running Total       : 260909151   Event Running Total   : 471

OAMLocalErrFrameSecsSummaryEvent : (ms = milliseconds)
---------------------------------------------------------------------------
Event Time Stamp : 3389
Errored Frame Second Summary Window     : 600(100ms)
Errored Frame Second Summary Threshold  : 1
Errored Frame Second Summary            : 60
Error Running Total       : 292         Event Running Total   : 5
```

Table 5 Command output

Field	Description
Port	Port index.
Link Status	Link status.
OAMLocalErrFrameEvent	Information about local errored frame events: • **Event Time Stamp**—Time when an errored frame event occurred (in 100 milliseconds). • **Errored Frame Window**—Error frame detection interval (in 100 milliseconds). • **Errored Frame Threshold**—Error threshold that triggers an errored frame event. • **Errored Frame**—Number of detected error frames over the specific detection interval. • **Error Running Total**—Total number of error frames. • **Event Running Total**—Total number of errored frame events that have occurred.
OAMLocalErrFramePeriodEvent	Information about local errored frame period events: • **Event Time Stamp**—Time when an errored frame event occurred (in 100 milliseconds). • **Errored Frame Window**—Maximum number of 64-byte frames that can be transmitted through an Ethernet port over the configured error frame period detection interval. For more information, see the "oam errored-frame-period period" command. • **Errored Frame Threshold**—Error threshold that triggers an error frame period event. • **Errored Frame**—Number of detected error frames over a detection interval. • **Error Running Total**—Total number of error frames that have detected. • **Event Running Total**—Total number of error frame period events.

Field	Description
OAMLocalErrFrameSecsSummaryEvent	Information about local errored frame seconds events: • **Event Time Stamp**—Time when an error frame seconds event occurred (in terms of 100 milliseconds). • **Errored Frame Second Summary Window**—Error frame second detection interval (in 100 milliseconds). • **Errored Frame Second Summary Threshold**—Error threshold that triggers an error frame seconds event. • **Errored Frame Second Summary**—Number of detected error frame seconds over a detection interval. • **Error Running Total**—Total number of error frame seconds. • **Event Running Total**—Total number of error frame seconds events that have occurred.

# Display remote Ethernet OAM link event statistics for all ports.

```
<Sysname> display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
---------------------------------------------------------------------
Event Time Stamp          : 5789       Errored Frame Window   : 10(100ms)
Errored Frame Threshold   : 1          Errored Frame         : 3
Error Running Total       : 35         Event Running Total   : 17
```

Table 6 Command output

Field	Description
Port	Port index
Link Status	Link status
OAMLocalErrFrameEvent	Information about remote errored frame events. • **Event Time Stamp**—Time when an errored frame event occurred (in 100 milliseconds). • **Errored Frame Window**—Error frame detection interval (in 100 milliseconds). • **Errored Frame Threshold**—Error threshold that triggers an errored frame event. • **Errored Frame**—Number of detected error frames over the specific detection interval. • **Error Running Total**—Total number of error frames. • **Event Running Total**—Total number of errored frame events that have occurred.

oam enable

Syntax

oam enable

undo oam enable

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **oam enable** to enable Ethernet OAM on the Ethernet port.

Use **undo oam enable** to disable Ethernet OAM on the Ethernet port.

By default, Ethernet OAM is disabled on all Ethernet ports.

Examples

# Enable OAM on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam enable
```

oam errored-frame period

Syntax

oam errored-frame period *period-value*

undo oam errored-frame period

View

System view

Default level

2: System level

Parameters

period-value: Errored frame event detection interval, ranging from 1 to 60 (in seconds).

Description

Use **oam errored-frame period** to set the errored frame event detection interval.

Use **undo oam errored-frame period** to restore the default.

By default, the errored frame event detection interval is one second.

Related commands: **oam errored-frame threshold**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame event detection interval to 10 seconds.

```
<Sysname> system-view
[Sysname] oam errored-frame period 10
```

oam errored-frame threshold

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Errored frame event triggering threshold, ranging from 0 to 4294967295.

Description

Use **oam errored-frame threshold** to set the errored frame event triggering threshold.

Use **undo oam errored-frame threshold** to restore the default.

By default, the errored frame event triggering threshold is 1.

Related commands: **oam errored-frame period**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame threshold 100
```

oam errored-frame-period period

Syntax

oam errored-frame-period period *period-value*

undo oam errored-frame-period period

View

System view

Default level

2: System level

Parameters

period-value: Errored frame period event detection interval, ranging from 100 to 60000 (in milliseconds).

Description

Use **oam errored-frame-period period** to set the errored frame period event detection interval.

Use **undo oam errored-frame-period period** to restore the default.

By default, the errored frame period event detection interval is 1000 milliseconds.

For errored frame period event detection, the system first uses the following expression to convert the errored frame period event detection interval to the maximum number of 64-byte frames that can be transmitted through an Ethernet port in the period:

bandwidth * period / (64 * 8 * 1000),

where **bandwidth** is the port bandwidth (in bps) and "period" is the configured period (in milliseconds).

Related commands: **oam errored-frame-period threshold**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame period event detection interval to 10 seconds (10000 milliseconds).

```
<Sysname> system-view
[Sysname] oam errored-frame-period period 10000
```

oam errored-frame-period threshold

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Errored frame period event triggering threshold, ranging from 0 to 4294967295.

Description

Use **oam errored-frame-period threshold** to set the errored frame period event triggering threshold.

Use **undo oam errored-frame-period threshold** to restore the default.

By default, the errored frame period event triggering threshold is 1.

Related commands: **oam errored-frame-period period**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame period event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame-period threshold 100
```

oam errored-frame-seconds period

Syntax

oam errored-frame-seconds period *period-value*

undo oam errored-frame-seconds period

View

System view

Default level

2: System level

Parameters

period-value: Errored frame seconds event detection interval, ranging from 10 to 900 (in seconds).

Description

Use **oam errored-frame-seconds period** to set the errored frame seconds event detection interval.

Use **undo oam errored-frame-seconds period** to restore the default.

By default, the errored frame seconds event detection interval is 60 seconds.

Related commands: **oam errored-frame-seconds threshold**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame seconds event detection interval to 100 seconds.

```
<Sysname> system-view
[Sysname] oam errored-frame-seconds period 100
```

oam errored-frame-seconds threshold

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Errored frame seconds event triggering threshold, ranging from 0 to 900.

Description

Use **oam errored-frame-seconds threshold** to set the errored frame seconds event triggering threshold.

Use **undo oam errored-frame-seconds threshold** to restore the default.

By default, the errored frame seconds event triggering threshold is 1.

Related commands: **oam errored-frame-seconds period**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored frame seconds event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame-seconds threshold 100
```

oam errored-symbol period

Syntax

oam errored-symbol period *period-value*

undo oam errored-symbol period

View

System view

Default level

2: System level

Parameters

period-value: Errored symbol event detection interval, ranging from 1 to 60 (in seconds).

Description

Use **oam errored-symbol period** to set the errored symbol event detection interval.

Use **undo oam errored-symbol period** to restore the default.

By default, the errored symbol event detection interval is one second.

Related commands: **oam errored-symbol threshold**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored symbol event detection interval to 10 seconds.

```
<Sysname> system-view
[Sysname] oam errored-symbol period 10
```

oam errored-symbol threshold

Syntax

oam errored-symbol threshold *threshold-value*

undo oam errored-symbol threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Errored symbol event triggering threshold, ranging from 0 to 4,294,967,295.

Description

Use **oam errored-symbol threshold** to set the errored symbol event triggering threshold.

Use **undo oam errored-symbol threshold** to restore the default.

By default, the errored symbol event triggering threshold is 1.

Related commands: **oam errored-symbol period**, **display oam link-event**, and **display oam configuration**.

Examples

# Set the errored symbol event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-symbol threshold 100
```

oam loopback

Syntax

oam loopback

undo oam loopback

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **oam loopback** to enable Ethernet OAM remote loopback on the specified Ethernet port.

Use **undo oam loopback** to disable Ethernet OAM remote loopback on the Ethernet port.

By default, Ethernet OAM remote loopback is disabled on the Ethernet port.

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

Related commands: **oam enable**, **oam loopback interface**, and **oam mode**.

Examples

# Configure the active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1, and then enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1 in Layer 2 Ethernet interface view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] oam loopback
```

oam loopback interface

Syntax

oam loopback interface *interface-type interface-number*

undo oam loopback interface *interface-type interface-number*

View

User view, system view

Default level

2: System level (command in system view)

1: Monitor level (command in user view)

Parameters

interface-type interface-number: Specifies a port by its type and number.

Description

Use **oam loopback interface** to enable Ethernet OAM remote loopback on an Ethernet port.

Use **undo oam loopback interface** to disable Ethernet OAM remote loopback on an Ethernet port.

By default, Ethernet OAM remote loopback is disabled on an Ethernet port.

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

Related commands: **oam enable**, **oam loopback**, and **oam mode**.

Examples

# Configure the active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1, and then enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1 in system view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname]oam loopback interface gigabitethernet 1/0/1
```

oam loopback reject-request

Syntax

oam loopback reject-request

undo oam loopback reject-request

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **oam loopback reject-request** to configure a port to reject the Ethernet OAM remote loopback request from a remote port.

Use **undo oam loopback reject-request** to restore the default.

By default, a port does not reject the Ethernet OAM remote loopback request from a remote port.

Examples

# Configure GigabitEthernet 1/0/1 to reject the Ethernet OAM remote loopback request from a remote port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam loopback reject-request
```

oam mode

Syntax

oam mode { **active** | **passive** }

undo oam mode

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

active: Specifies the active Ethernet OAM mode.

passive: Specifies the passive Ethernet OAM mode.

Description

Use **oam mode** to set the Ethernet OAM mode for an Ethernet port.

Use **undo oam mode** to restore the default.

By default, an Ethernet OAM-enabled Ethernet port operates in the active Ethernet OAM mode.

To change the Ethernet OAM mode of an Ethernet OAM-enabled Ethernet port, you need to disable Ethernet OAM on the port first.

Related commands: **oam enable**.

Examples

# Disable Ethernet OAM on GigabitEthernet 1/0/1, and then configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo oam enable
[Sysname-GigabitEthernet1/0/1] oam mode passive
```

oam timer hello

Syntax

oam timer hello *interval*

undo oam timer hello

View

System view

Default level

2: System level

Parameters

interval: Ethernet OAM handshake packet transmission interval, in milliseconds. The value of this argument must be a multiple of 100 and range from 500 to 5000. .

Description

Use **oam timer hello** to configure the Ethernet OAM handshake packet transmission interval.

Use **undo oam timer hello** to restore the default.

By default, the Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

After the timeout timer for an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to be disconnected. HP recommends setting the connection timeout timer at least five times the handshake packet transmission interval, ensuring the stability of Ethernet OAM connections.

Related commands: **oam timer keepalive** and **display oam configuration**.

Examples

# Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds—assume that the Ethernet OAM connection timeout timer is 5000 milliseconds.

```
<Sysname> system-view
[Sysname] oam timer hello 600
```

oam timer keepalive

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

View

System view

Default level

2: System level

Parameters

interval: Ethernet OAM connection timeout timer, in milliseconds. The value of this argument must be a multiple of 100 and range from 1000 to 25000.

Description

Use **oam timer keepalive** to configure the Ethernet OAM connection timeout timer.

Use **undo oam timer keepalive** to restore the default.

By default, the Ethernet OAM connection timeout timer is 5000 milliseconds.

After the timeout timer for an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to be disconnected. HP recommends setting the connection timeout timer at least five times the handshake packet transmission interval, ensuring the stability of Ethernet OAM connections.

Related commands: **oam timer hello** and **display oam configuration**.

Examples

# Set the Ethernet OAM connection timeout timer to 6000 milliseconds—assume that the Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

```
<Sysname> system-view
[Sysname] oam timer keepalive 6000
```

reset oam

Syntax

reset oam [**interface** *interface-type interface-number*]

View

User view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use **reset oam** to clear the Ethernet OAM packet and link error event statistics for the specified port or all ports.

If no port is specified, this command clears the Ethernet OAM packet and link error event statistics for all ports.

Related commands: **display oam** and **display oam link-event**.

Examples

# Clear Ethernet OAM packet and link error event statistics for all ports.

```
<Sysname> reset oam
```

CFD configuration commands

cfd ais enable

Syntax

cfd ais enable

undo cfd ais enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **cfd ais enable** to enable AIS.

Use **undo cfd ais enable** to disable AIS.

By default, AIS is disabled.

Examples

# Enable AIS.

```
<Sysname> system-view
[Sysname] cfd ais enable
```

cfd ais level

Syntax

cfd ais level *level-value* **service-instance** *instance-id*

undo cfd ais level *level-value* **service-instance** *instance-id*

View

System view

Default level

2: System level

Parameters

level *level-value*: Specifies the AIS frame transmission level, which ranges from 1 to 7.

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

Description

Use **cfd ais level** to configure the AIS frame transmission level in the specified service instance.

Use **undo cfd ais level** to restore the default.

By default, no AIS frame transmission level is configured for a service instance.

If no AIS frame transmission level is configured for a service instance, the MEPs in the service instance cannot send AIS frames.

Regardless of the value of the *level-value* argument, the **undo cfd ais level** command restores the AIS frame transmission level to an invalid value.

Examples

# Configure the AIS frame transmission level as 3 in service instance 1.

```
<Sysname> system-view
[Sysname] cfd ais level 3 service-instance 1
```

cfd ais period

Syntax

cfd ais period *period-value* **service-instance** *instance-id*

undo cfd ais period *period-value* **service-instance** *instance-id*

View

System view

Default level

2: System level

Parameters

period *period-value*: Specifies the AIS frame transmission period, which ranges from 1 to 60 seconds.

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

Description

Use **cfd ais period** to configure the AIS frame transmission period in the specified service instance.

Use **undo cfd ais period** to restore the default.

By default, the AIS frame transmission period is 1 second in all service instances.

Regardless of the value of the *period-value* argument, the **undo cfd ais period** command restores the AIS frame transmission period to 1 second.

Examples

# Configure the AIS frame transmission period as 60 seconds in service instance 1.

```
<Sysname> system-view
[Sysname] cfd ais period 60 service-instance 1
```

cfd cc enable

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use **cfd cc enable** to enable CCM sending on a specified MEP.

Use **undo cfd cc enable** to disable CCM sending on a specified MEP.

By default, the CCM sending function is disabled.

Related commands: **cfd cc interval**.

Examples

# On port GigabitEthernet 1/0/1, enable CCM sending on MEP 3 in service instance 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable
```

cfd cc interval

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

interval *interval-value*: Specifies the value of the interval field in CCM messages, which ranges from 4 to 7.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

Description

Use **cfd cc interval** to set the value of the interval field in the CCM messages.

Use **undo cfd cc interval** to restore default.

By default, the value of this field is 4 for all CCMs sent.

The relationship between the interval field value in the CCM messages, the interval for sending CCM messages, and the timeout time of the remote MEP is shown in Table 7.

Table 7 Relationship of interval field value, interval for sending CCMs, and timeout time of remote MEP

Interval field value	Interval for sending CCMs	Timeout time of remote MEP
4	1 second	3.5 seconds

Interval field value	Interval for sending CCMs	Timeout time of remote MEP
5	10 seconds	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Related commands: **cfd cc enable**.

Examples

# Set the value of the interval field in CCMs sent by MEPs in service instance 2 to 7.

```
<Sysname> system-view
[Sysname] cfd cc interval 7 service-instance 2
```

cfd dm one-way

Syntax

cfd dm one-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number *number*: Specifies the number of 1DM frames sent. The *number* argument ranges from 2 to 10, and defaults to 5.

Description

Use **cfd dm one-way** to enable one-way DM. The one-way DM function measures the one-way frame delay between two MEPs by sending 1DM frames from the source MEP to the target MEP.

By default, one-way DM is disabled.

The one-way DM function takes effect only in CFD IEEE 802.1ag.

To view the one-way delay test result, use the **display cfd dm one-way history** command on the target MEP.

Related commands: **cfd version** and **display cfd dm one-way history**.

Examples

# Enable the one-way DM function in CFD IEEE 802.1ag to test the one-way frame delay from source MEP 1101 to target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1.

```
<Sysname> system-view
[Sysname] cfd version standard
```

```
[Sysname] cfd dm one-way service-instance 1 mep 1101 target-mep 2001
Info: 5 1DMs have been sent. Please check the result on the remote device.
```

cfd dm two-way

Syntax

cfd dm two-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number *number*: Specifies the number of DMM frames sent. The *number* argument ranges from 2 to 10, and defaults to 5.

Description

Use **cfd dm two-way** to enable two-way DM. The two-way DM function measures the two-way frame delay between two MEPs by sending DMM frames from the source MEP to the target MEP and detecting the responded DMR frames.

By default, two-way DM is disabled.

The two-way DM function takes effect only in CFD IEEE 802.1ag.

Related commands: **cfd version**.

Examples

# Enable the two-way DM function in CFD IEEE 802.1ag to test the two-way frame delay between source MEP 1101 and target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd dm two-way service-instance 1 mep 1101 target-mep 2001
Frame delay:
Reply from 0010-FC00-6512: 10ms
Reply from 0010-FC00-6512: 9ms
Reply from 0010-FC00-6512: 11ms
Reply from 0010-FC00-6512: 5ms
Reply from 0010-FC00-6512: 5ms
Average: 8ms
Send DMMs: 5       Received: 5       Lost: 0

Frame delay variation: 5ms  4ms  6ms  0ms  0ms
Average: 3ms
```

Table 8 Command output

Field	Description
Reply from 0010-FC00-6512	Delay of the DMR frames returned from the MEP with MAC address 0010-FC00-6512
Average	Average frame delay or average frame delay variation
Send DMMs	Number of DMM frames sent
Received	Number of DMM frames received
Lost	Number of DMM frames lost

cfd enable

Syntax

cfd enable

undo cfd enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **cfd enable** to enable CFD.

Use **undo cfd enable** to disable CFD.

By default, CFD is disabled.

Examples

# Enable CFD.

```
<Sysname> system-view
[Sysname] cfd enable
```

cfd linktrace

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]

View

Any view

Default level

0: Visit level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of the source MEP, ranging from 1 to 8191.

target-map *target-mep-id*: Specifies the ID of the destination MEP, ranging from 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

ttl *ttl-value*: Specifies the time to live value, ranging from 1 to 255 and defaulting to 64.

hw-only: Sets the hw-only bits of the LTMs sent. When this keyword is specified and the MIP that receives LTMs cannot find the destination MAC address in its forwarding table, the MIP does not broadcast these LTM messages. Otherwise, the MIP forwards these LTM messages.

Description

Use **cfd linktrace** to find the path between the source and target MEPs, which is achieved through the transmission of LTMs between the two and detection of the responding LTRs.

Related commands: **cfd linktrace auto-detection**.

Examples

# Identify the path between source MEP 1101 and target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1 when the standard version (IEEE 802.1ag) of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361
MAC Address               TTL     Last MAC         Relay Action
0010-FC00-6512            63      0010-FC00-6500   Hit
```

# Identify the path between source MEP 1101 and target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1 when the IEEE 802.1ag draft 5.2 version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5
[Sysname] cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361 :
MAC Address               TTL     Forwarded          Relay Action
0010-FC00-6512            63      No                 None
```

# Identify the path between source MEP 1101 and target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1 when the IEEE 802.1ag draft 5.2 interim version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5-plus
[Sysname] cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361 :
MAC Address               TTL     Forwarded          Relay Action
0010-FC00-6512            63      No                 None
```

NOTE:

The output varies by CFD protocol version.

Table 9 Command output

Field	Description
Linktrace to MEP 2001 with the sequence number 1101-43361	Linktrace to target MEP 2001 with the sequence number 1101-43361.
MAC Address	Source MAC address in the LTR messages.
TTL	Hop count when the LTM passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Forwarded	Indicates whether the device forwards LTMs: • Yes means that the current device forwards LTMs. • No means that the current device does not forward LTMs.
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or that the destination MAC address is found in the MEP or MIP database. When the IEEE 802.1ag draft5.2 version or the IEEE 802.1ag draft 5.2 interim version of CFD is used: • **Found**—The forwarding device found the destination MAC address. • **Unknown**—The forwarding device failed to find the destination MAC address. • **None**—It is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

cfd linktrace auto-detection

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

View

System view

Default level

2: System level

Parameters

size *size-value*: Specifies the size of the buffer used to store the auto-detection result, ranging from 1 to 100 (in terms of sending times).

This value defaults to 5, which means the buffer stores the results of the recent five auto-detections.

Description

Use **cfd linktrace auto-detection** to enable the auto sending of linktrace messages.

Use **undo cfd linktrace auto-detection** to disable this function.

By default, this function is disabled.

After LT messages automatic sending is enabled, if the source MEP fails to receive the CCMs from the target MEP within 3.5 times the sending interval, the link between the two is regarded as faulty and LTMs will be sent out. (The destination of the LTMs is the target MEP, and the TTL field value is 255.) Based on the LTRs that echo back, the fault source can be located.

Once you disable LT messages automatic sending, the content stored in the buffer will be removed.

Related commands: **cfd linktrace**.

Examples

# Enable automatic LT messages sending, and specify the size of the buffer used to store the auto-detection result to 100 (in terms of sending times).

```
<Sysname> system-view
[Sysname] cfd linktrace auto-detection size 100
```

cfd loopback

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *number*]

View

Any view

Default level

0: Visit level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

target-mep *target-mep-id*: Specifies the ID of the target MEP for LBM packets, ranging from 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

number *number*: Specifies the number of the LBMs packets sent, ranging from 1 to 10 and defaulting to 5.

Description

Use **cfd loopback** to enable LB function so that LBMs can be sent from the specified MEP to other MPs in the same service instance, and LBR messages can be received.

By default, LB is not enabled.

Examples

# Enable LB to check the status of the link between MEP 1101 and MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1 (assume that the link status is normal).

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to 0010-FC00-6512 with the sequence number start from 1101-43404:
Reply from 0010-FC00-6512: sequence number=1101-43404 time=5ms
Reply from 0010-FC00-6512: sequence number=1101-43405 time=5ms
Reply from 0010-FC00-6512: sequence number=1101-43406 time=5ms
Reply from 0010-FC00-6512: sequence number=1101-43407 time=5ms
Reply from 0010-FC00-6512: sequence number=1101-43408 time=5ms
```

```
Send:5         Received:5        Lost:0
```

# Enable LB to check the status of the link between MEP 1101 and MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1 (assume that the link status is abnormal).

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Sequence number=1101-43404: Request timed out
Sequence number=1101-43404: Request timed out
Sequence number=1101-43404: Request timed out
Sequence number=1101-43404: Request timed out
Sequence number=1101-43404: Request timed out
Send:5         Received:0        Lost:5
```

Table 10 Command output

Field	Description
Loopback to 0010-FC00-6512 with the sequence number start from 1101-43404	Sends LBMs to 0010-FC00-6512 with the sequence number starting with 1101-43404.
sequence number	Sequence number in the LBR messages.
time=5ms	The interval between the sending of LBMs and receiving of LBRs is 5 milliseconds.
Request timed out	The request is timed out because no LBR is received within 5 milliseconds.
Send	Number of LBMs sent.
Received	Number of LBR messages received.
Lost	Number of lost LBRs.

cfd ma

Syntax

cfd ma *ma-name* **md** *md-name* **vlan** *vlan-id*

undo cfd ma *ma-name* **md** *md-name*

View

System view

Default level

2: System level

Parameters

ma *ma-name*: Specifies the name of the MA, a string of 1 to 43 characters. IEEE 802.1ag standard version allows an MA name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MA name to contain letters, numbers, and special characters (including – and _), but do not allow an MA name to start or end with a special character.

md *md-name*: Specifies the name of an MD, a string of 1 to 43 characters. IEEE 802.1ag standard version allows an MD name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MD name to contain letters, numbers, and special characters (including – and _), but do not allow an MD name to start or end with a special character.

vlan *vlan-id*: Specifies the ID of the VLAN where MA is in service, ranging from 1 to 4094.

Description

Use **cfd ma** to create MAs in an MD.

Use **undo cfd ma** to delete MAs in an MD.

By default, no MA is created.

Before creating an MA, you must create an MD first.

The total length of the MA and MD names should not exceed 44 characters.

Deleting an MA also deletes the configurations related to that MA.

Related commands: **cfd md**.

Examples

# Create an MA named **test_ma** in an MD named **test_md**, and configure the MA to serve VLAN 100.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
```

cfd md

Syntax

cfd md *md-name* **level** *level-value*

undo cfd md *md-name*

View

System view

Default level

2: System level

Parameters

md *md-name*: Specifies the name of an MD, a string of 1 to 43 characters. IEEE 802.1ag standard version allows an MD name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MD name to contain letters, numbers, and special characters (including – and _), but do not allow an MD name to start or end with a special character.

level *level-value*: Specifies an MD level, ranging from 0 to 7.

Description

Use **cfd md** to create an MD.

Use **undo cfd md** to delete an MD.

By default, no MD is created.

You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name.

Deleting an MD also deletes the configurations related to that MD.

Examples

# Create an MD named **test_md**, with its level being 3.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
```

cfd mep

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

inbound: Creates an inward-facing MEP.

outbound: Creates an outward-facing MEP.

Description

Use **cfd mep** to create a MEP on a port.

Use **undo cfd mep** to delete the specified MEP.

By default, no MEP exists on a port.

In creating a MEP, the service instance you specified defines the MD and MA that the MEP belongs to.

You cannot create a MEP if the MEP ID is not included in the MEP list of the relevant service instance.

Related commands: **cfd meplist**.

Examples

# Configure a MEP list in service instance 5, and create and enable inward-facing MEP 3 in service instance 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
[Sysname] cfd meplist 3 service-instance 5
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd mep 3 service-instance 5 inbound
```

cfd mep enable

Syntax

cfd mep service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd mep service-instance *instance-id* **mep** *mep-id* **enable**

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use **cfd mep enable** to enable the MEP configured on a port.

Use **undo cfd mep enable** to disable the MEP.

By default, MEP is disabled on a port and cannot respond to various CFD frames (such as LTM frames, LBM frames, 1DM frames, DMM frames, and TST frames) unless you enable it.

Related commands: **cfd mep**.

Examples

# Enable MEP 3 in service instance 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd mep service-instance 5 mep 3 enable
```

cfd meplist

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

View

System view

Default level

2: System level

Parameters

meplist *mep-list*: Specifies a list of MEP IDs. The *mep-list* argument takes the form of { *mep-id* [**to** *mep-id*] }&<1-10>, where *mep-id* represents the MEP ID and ranges from 1 to 8191. *&<1-10>* indicates you can specify up to 10 MEP ID ranges.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

Description

Use **cfd meplist** to create a MEP list, which is a collection of local MEPs allowed to be configured and the remote MEPs to be monitored in the same MA.

Use **undo cfd meplist** to delete existing MEP lists.

By default, no MEP list is created.

Before creating a MEP list, create the relevant MD, MA, and service instance.

After you delete a MEP list, all local MEP configurations based on this list are deleted.

Related commands: **cfd ma**, **cfd md**, and **cfd service-instance**.

Examples

# Create a MEP list that includes MEP 9 through MEP 15 in service instance 5.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
[Sysname] cfd meplist 9 to 15 service-instance 5
```

cfd mip-rule

Syntax

cfd mip-rule { **explicit** | **default** } **service-instance** *instance-id*

undo cfd mip-rule service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

explicit: This rule means that if the lower level MA is not configured with MIPs, whether the current MA will create MIPs depends on whether the lower level MA is configured with MEPs.

default: This rule means that if the lower level MA is not configured with MIPs, the current MA will create MIPs.

Description

Use **cfd mip-rule** to configure the rules for generating MIPs. MIPs are generated on each port automatically according to the rules configured.

Use **undo cfd mip-rule** to delete the rule for generating MIPs.

By default, no rules for generating MIPs are configured and no MIPs exist.

Examples

# Configure the MIP generation rule as default in service instance 5.

```
<Sysname> system-view
[Sysname] cfd mip-rule default service-instance 5
```

cfd service-instance

Syntax

cfd service-instance *instance-id* **md** *md-name* **ma** *ma-name*

undo cfd service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

md *md-name*: Specifies the name of an MD. The *md-name* argument is a string of 1 to 43 characters. IEEE 802.1ag standard version allows an MD name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MD name to contain letters, numbers, and special characters (including – and _), but do not allow an MD name to start or end with a special character.

ma *ma-name*: Specifies the name of an MA. The *ma-name* argument is a string of 1 to 43 characters. IEEE 802.1ag standard version allows an MA name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MA name to contain letters, numbers, and special characters (including – and _), but do not allow an MA name to start or end with a special character.

Description

Use **cfd service-instance** to create a service instance with the MD name.

Use **undo cfd service-instance** to delete a service instance.

By default, no service instance is created.

You must create the relevant MD and MA prior to creating a service instance with the MD name.

The service instance ID uniquely identifies an MA in an MD.

When deleting a service instance, you are deleting the configurations related to that service instance as well.

Deleting a service instance simply breaks up the connection between the service instance and the relevant MA, the MA itself is not deleted.

A service instance with the MD name takes effect in all versions of CFD.

Related commands: **cfd md**, **cfd ma**, and **cfd version**.

Examples

# Create a level-3 MD named **test_md**, create an MA named **test_ma**, which serves VLAN 100, in **test_md**, and then create service instance 5 with the MD name for **test_md** and **test_ma**.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
```

cfd service-instance maid format

Syntax

cfd service-instance *instance-id* **maid format** { **icc-based** *ma-name* | **string** *ma-name* } **level** *level-value* **vlan** *vlan-id*

undo cfd service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

icc-based *ma-name*: MA name in the Y.1731 format. The *ma-name* argument is a string of 1 to 13 characters. IEEE 802.1ag standard version allows an MA name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MA name to contain letters, numbers, and special characters (including – and _), but do not allow an MA name to start or end with a special character.

string *ma-name*: MA name in the IEEE 802.1ag format. The *ma-name* argument is a string of 1 to 45 characters. IEEE 802.1ag standard version allows an MA name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MA name to contain letters, numbers, and special characters (including – and _), but do not allow an MA name to start or end with a special character.

level *level-value*: Specifies the MD level for the service instance, which ranges from 0 to 7.

vlan *vlan-id*: Specifies the VLAN for the service instance. The *vlan-id* argument ranges from 1 to 4094.

Description

Use **cfd service-instance maid format** to create a service instance without the MD name.

Use **undo cfd service-instance** to remove the specified service instance.

By default, no service instance is created.

When you create a service instance without the MD name, the system automatically creates the MA and MD for the service instance.

The service instance ID, MA name, and MD level uniquely identify a MA.

Deleting a service instance also deletes all configurations based on the service instance.

Deleting a service instance removes not only the service instance ID-MA association, but also the MA.

A MD with no MAs will be deleted.

A service instance without the MD name takes effect only in the IEEE 802.1ag standard version of CFD.

Related commands: **cfd version**.

Examples

# Create service instance 5 without the MD name in CFD IEEE 802.1ag, and configure the MA named **test_ma1** in the Y.1731 format, MD level 3, and VLAN 100 for the service instance.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd service-instance 5 maid format icc-based test_ma1 level 3 vlan 100
```

# Create service instance 6 without the MD name in CFD IEEE 802.1ag, and configure the MA named **test_ma2** in the IEEE 802.1ag format, MD level 4, and VLAN 200 for the service instance.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd service-instance 6 maid format string test_ma2 level 4 vlan 200
```

cfd slm

Syntax

cfd slm service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number *number*: Specifies the number of LMM frames sent. The *number* argument ranges from 2 to 10, and defaults to 5.

Description

Use **cfd slm** to enable LM. The LM function measures the frame loss between two MEPs by sending LMM frames from the source MEP to the target MEP and detecting the returned LMR frames.

By default, LM is disabled.

The LM function takes effect only in CFD IEEE 802.1ag.

Related commands: **cfd version**.

Examples

# Enable the LM function in CFD IEEE 802.1ag to measure the frame loss between source MEP 1101 and target MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd slm service-instance 1 mep 1101 target-mep 2001
Reply from 0010-FC00-6512
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-FC00-6512
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-FC00-6512
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-FC00-6512
Far-end frame loss: 30    Near-end frame loss: 30

Average
Far-end frame loss: 20    Near-end frame loss: 25
Far-end frame loss rate: 25%    Near-end frame loss rate: 32%
Send LMMs: 5        Received: 5        Lost: 0
```

Table 11 Command output

Field	Description
Reply from 0010-FC00-6512	LMR frames returned from the target MEP with MAC address 0010-FC00-6512
Far-end frame loss	Number of lost frames on the target MEP
Near-end frame loss	Number of lost frames on the source MEP
Far-end frame loss rate	Average frame loss ratio on the target MEP
Near-end frame loss rate	Average frame loss ratio on the source MEP
Average	Average number of lost frames
Send LMMs	Number of LMM frames sent
Received	Number of LMR frames received
Lost	Number of LMR frames lost

cfd tst

Syntax

cfd tst service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*] [**length-of-test** *length*] [**pattern-of-test** { **all-zero** | **prbs** } [**with-crc**]]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number *number*: Specifies the number of TST frames sent. The *number* argument ranges from 1 to 10, and defaults to 5.

length-of-test *length*: Specifies the length of the Test TLV (Type/Length/Value) in the TST frame. The *length* argument ranges from 4 to 1400 and defaults to 64.

pattern-of-test { all-zero | prbs } [with-crc]: Specifies the pattern of the Test TLV in the TST frame, which can be **all-zero** (all-zero value without CRC-32), **prbs** (pseudo random bit sequence without CRC-32), **all-zero with-crc** (all-zero value with CRC-32), and **prbs with-crc** (pseudo random bit sequence with CRC-32). The default mode is **all-zero**.

Description

Use **cfd tst** to enable the TST function. The TST function detects the bit errors between two MEPs by sending TST frames from the source MEP to the target MEP.

By default, the TST function is disabled.

The TST function takes effect only in CFD IEEE 802.1ag.

To view the TST test result, use the **display cfd tst** command on the target MEP.

Related commands: **cfd version** and **display cfd tst**.

Examples

# Enable the TST function in CFD IEEE 802.1ag to test the bit errors between source MEP 1101 and destination MEP 2001 (whose MAC address is 0010-FC00-6512) in service instance 1.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] cfd tst service-instance 1 mep 1101 target-mep 2001
Info: TST process is done. Please check the result on the remote device.
```

Table 12 Command output

Field	Description
TST process is done	The TST test has been performed

cfd version

Syntax

cfd version { **draft5** | **draft5-plus** | **standard** }

undo cfd version

View

System view

Default level

2: System level

Parameters

draft5: Specifies that IEEE 802.1ag draft5.2 be used.

draft5-plus: Specifies that the IEEE 802.1ag draft5.2 interim version be used.

standard: Specifies that the standard version of IEEE 802.1ag be used.

Description

Use **cfd version** to configure the CFD protocol version.

Use **undo cfd version** to restore the default.

By default, CFD uses the standard version of IEEE 802.1ag.

If an MD is created by using the **cfd md** command or automatically generated by using the **cfd service-instance maid format** command on a device, you cannot switch between the standard and non-standard versions (draft5.2 version and draft5.2 interim version), however, you can switch between the draft5.2 version and draft5.2 interim version. This restriction does not apply to the device without an MD configured.

Related commands: **cfd md** and **cfd service-instance maid format**.

Examples

# Configure the CFD protocol version as IEEE 802.1ag draft5.2.

```
<Sysname> system-view
[Sysname] cfd version draft5
```

display cfd ais

Syntax

display cfd ais [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the MEP by its ID, which ranges from 1 to 8191.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd ais** to display the AIS configuration and information on the specified MEP.

If no MEP is specified, the **display cfd ais** command displays the AIS configuration and information of all MEPs in the specified service instance.

If no service instance is specified, the **display cfd ais** command displays the AIS configuration and information of all MEPs in all service instances.

Related commands: **cfd ais enable**, **cfd ais level**, and **cfd ais period**.

Examples

# Display the AIS configuration and information of all the MEPs in all service instances.

```
<Sysname> display cfd ais
Service instance: 5
AIS level: 4    AIS period: 1s
MEP ID: 1
AIS condition: yes   Time to enter the condition: 2009/05/22 10:43:57
AIS state machine: Prestate: NO_RECEIVE
                   Curstate: RECEIVE
MEP ID: 2
AIS condition: yes   Time to enter the condition: 2009/05/22 10:43:57
AIS state machine: Prestate: NO_RECEIVE
                   Curstate: RECEIVE
```

```
Service instance: 20
AIS level: 3    AIS period: 60s
MEP ID: 10
AIS condition: yes   Time to enter the condition: 2009/05/22 10:43:57
AIS state machine: Prestate: NO_RECEIVE
                   Curstate: RECEIVE

Service instance: 100
AIS level: 6    AIS period: 1s
MEP ID: 20
AIS condition: no    Time to enter the condition: 2006/05/22 11:40:01
AIS state machine: Prestate: IDLE
                   Curstate: NO_RECEIVE
```

Table 13 Command output

Field	Description
Service instance	Service instance of the MEP.
AIS level	AIS frame transmission level.
AIS period	AIS frame transmission period.
AIS condition	AIS status: • **yes**—AIS is running. • **no**—AIS is not running.
Time to enter the condition	Time when the AIS status began.
AIS state machine	AIS packet receiving state machine.
Prestate	Previous state: • **IDLE**—Not activated. • **NO_RECEIVE**—Activated. • **RECEIVE**—AIS frames are received.
Curstate	Current state: • **IDLE**—Not activated. • **NO_RECEIVE**—Activated. • **RECEIVE**—AIS frames are received.

display cfd dm one-way history

Syntax

display cfd dm one-way history [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the MEP by its ID, which ranges from 1 to 8191.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd dm one-way history** to display the one-way DM result on the specified MEP.

If no MEP is specified, the **display cfd dm one-way history** command displays the one-way DM results of all MEPs in the specified service instance.

If no service instance is specified, the **display cfd dm one-way history** command displays the one-way DM results of all MEPs in all service instances.

Related commands: **cfd dm one-way**.

Examples

# Display the one-way DM results of all the MEPs in all service instances.

```
<Sysname> display cfd dm one-way history
Service instance: 1
MEP ID: 1003
Send 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms  9ms  11ms  5ms  5ms
Delay average: 8ms
Frame delay variation:5ms  4ms  6ms  0ms 0ms
Variation average: 3ms
MEP ID: 1004
Send 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms  9ms  11ms  5ms  5ms
Delay average: 8ms
Delay variation: 5ms  4ms  6ms  0ms  0ms
Variation average: 3ms

Service instance: 2
No mep exists in the service instance.

Service instance: 3
MEP ID: 1023
Send 1DM total number: 5
Received 1DM total number: 10
Frame delay: 20ms  9ms  8ms  7ms  1ms 5ms  13ms  17ms  9ms  10ms
Delay average: 9ms
Delay variation: 19ms  8ms  7ms  6ms  0ms 4ms  12ms  16ms  8ms  9ms
Variation average: 8ms

Service instance: 4
MEP ID: 1023
Send 1DM total number: 77
Received 1DM total number: 0
```

Table 14 Command output

Field	Description
Service instance	Service instance of the MEP
Send 1DM total number	Number of 1DM frames sent
Received 1DM total number	Number of 1DM frames received
Delay average	Average frame delay
Delay variation	Frame delay variation
Variation average	Average frame delay variation

display cfd linktrace-reply

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd linktrace-reply** to display the LTR information received by a MEP.

If no MEP is specified, this command displays LTR information for all MEPs in the current service instance.

If no service instance is specified, this command displays LTR information for all MEPs.

Examples

# Display LTR information saved on all the MEPs in every service instance when the standard version (IEEE 802.1ag) of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] display cfd linktrace-reply
Service instance: 1       MEP ID: 1003
MAC Address               TTL     Last MAC          Relay Action
0000-FC00-6505            63      0000-FC00-6504    MPDB
000F-E269-A852            62      0000-FC00-6505    FDB
0000-FC00-6508            61      000F-E269-A852    Hit
Service instance: 2       MEP ID: 1023
MAC Address               TTL     Last MAC          Relay Action
0000-FC00-6508            61      000F-E269-A852    Hit
```

# Display the LTR information saved on all the MEPs in every service instance when the IEEE 802.1ag draft5.2 version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5
[Sysname] display cfd linktrace-reply
Service instance: 1       MEP ID: 1003
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      Yes               Found
00E0-FC00-6510            62      Yes               Found
00E0-FC52-BAA0            61      No                None

Service instance: 2       MEP ID: 1023
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      No                None
```

# Display the LTR information saved on all the MEPs in every service instance when the IEEE 802.1ag draft5.2 interim version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5-plus
[Sysname] display cfd linktrace-reply
Service instance: 1       MEP ID: 1003
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      Yes               Found
00E0-FC00-6510            62      Yes               Found
00E0-FC52-BAA0            61      No                None

Service instance: 2       MEP ID: 1023
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      No                None
```

NOTE:

The output varies by CFD protocol version.

Table 15 Command output

Field	Description
Service instance	Service instance to which the MEPs that send LTMs belong.
MEP ID	ID of the MEP that sends LTMs.
MAC Address	Source MAC address in the LTR message.
TTL	Hop count when LTM passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Forwarded	Indicates whether the device forwards LTMs: • Yes means that the device has forwarded the LTMs. • No means that the device did not forward the LTMs.
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—Indicates that the current device is the destination device. • **FDB**—Indicates that the forwarding device found the destination MAC address. • **MPDB**—Indicates that the destination MAC address is not found, or that the destination MAC address is found in the MEP or MIP database. When the IEEE 802.1ag draft5.2 version or the IEEE 802.1ag draft5.2 interim version of CFD is used: • **Found**—Indicates that the forwarding device found the destination MAC address in its MAC address table. • **Unknown**—Indicates that the forwarding device failed to find the destination MAC address in its MAC address table. • **None**—Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

display cfd linktrace-reply auto-detection

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

size *size-value*: Specifies the times of recent auto-detections, ranging from 1 to 100.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd linktrace-reply auto-detection** to display the content of the LTR messages received as responses to the automatically sent LTMs.

These LTR messages received as responses to automatically sent LTMs are stored in the buffer after you executed the **cfd linktrace auto-detection** command.

If no size is specified, this command displays information about all LTRs stored in the buffer.

Related commands: **cfd linktrace auto-detection**.

Examples

# Display the contents of the LTRs received as responses to the LTMs automatically sent when the standard version (IEEE 802.1ag) of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version standard
[Sysname] display cfd linktrace-reply auto-detection
Service instance: 1       MEP ID: 1003    Time: 2006/05/22 10:43:57
Target MEP ID: 2005       TTL: 64
MAC Address               TTL     Last MAC          Relay Action
0000-FC00-6505            63      0000-FC00-6504    MPDB
000F-E269-A852            62      0000-FC00-6505    FDB
0000-FC00-6508            61      000F-E269-A852    Hit
Service instance: 2       MEP ID: 1023    Time: 2006/05/22 10:44:06
Target MEP ID: 2025       TTL: 64
MAC Address               TTL     Last MAC          Relay Action
0000-FC00-6508            61      000F-E269-A852    Hit
```

# Display the contents of the LTRs received as responses to the LTMs automatically sent when the IEEE 802.1ag draft5.2 version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5
[Sysname] display cfd linktrace-reply auto-detection
Service instance: 1       MEP ID: 1003    Time: 2006/05/22 10:43:57
Target MEP ID: 2005       TTL: 64
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      Yes               Found
00E0-FC00-6510            62      Yes               Found
00E0-FC52-BAA0            61      No                None

Service instance: 2       MEP ID: 1023    Time: 2006/05/22 10:44:06
Target MEP ID: 2025       TTL: 64
MAC Address               TTL        Forwarded         Relay Action
00E0-FC27-6502            63         No                None
```

# Display the contents of the LTRs received as responses to the LTMs automatically sent when the IEEE 802.1ag draft5.2 interim version of CFD is used.

```
<Sysname> system-view
[Sysname] cfd version draft5-plus
[Sysname] display cfd linktrace-reply auto-detection
Service instance: 1       MEP ID: 1003    Time: 2006/05/22 10:43:57
```

```
Target MEP ID: 2005       TTL: 64
MAC Address               TTL     Forwarded         Relay Action
00E0-FC27-6502            63      Yes               Found
00E0-FC00-6510            62      Yes               Found
00E0-FC52-BAA0            61      No                None

Service instance: 2       MEP ID: 1023    Time: 2006/05/22 10:44:06
Target MEP ID: 2025       TTL: 64
MAC Address               TTL        Forwarded         Relay Action
00E0-FC27-6502            63         No                None
```

NOTE:

The output varies by CFD protocol version.

Table 16 Command output

Field	Description
Service instance	Service instance to which the MEPs that sent LTM messages belong.
MEP ID	ID of the MEP that sends LTMs.
Time	Time of the LTMs automatically sent.
Target MEP ID	ID of the target MEP.
TTL	Initial hop count of the automatically sent LTMs.
MAC Address	Source MAC address in the LTR messages.
TTL	Hop count when LTM passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Forwarded	Indicates whether the device forwards LTMs: • Yes means that the device has forwarded the LTMs. • No means that the device did not forward the LTMs.
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—Indicates that the current device is the destination device. • **FDB**—Indicates that the forwarding device found the destination MAC address. • **MPDB**—Indicates that the destination MAC address is not found, or that the destination MAC address is found in the MEP or MIP database. When the IEEE 802.1ag draft5.2 version or the IEEE 802.1ag draft5.2 interim version of CFD is used: • **Found**—Indicates that the forwarding device found the destination MAC address. • **Unknown**—Indicates that the forwarding device failed to find the destination MAC address. • **None**—Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

display cfd ma

Syntax

display cfd ma [[*ma-name*] **md** { *md-name* **|** **level** *level-value* }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ma-name: Name of MA, a character string of 1 to 43 characters. IEEE 802.1ag standard version allows an MA name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MA name to contain letters, numbers, and special characters (including – and _), but do not allow an MA name to start or end with a special character.

md-name: Name of an MD, a character string of 1 to 43 characters. IEEE 802.1ag standard version allows an MD name to contain letters, numbers, and special characters (including ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] | \ : ; " ' < > , . /). IEEE 802.1ag draft5.2 version and IEEE 802.1ag draft5.2 interim version allow an MD name to contain letters, numbers, and special characters (including – and _), but do not allow an MD name to start or end with a special character.

level *level-value*: MD level, which ranges from 0 to 7.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd ma** to display the configuration of a specified MA.

If MD is not specified, this command displays the MA configurations of all MDs on the device.

If both MD and MA are specified, this command displays the specified MA configuration.

If only MD is specified, this command displays the configurations of all MAs in that MD.

If an MD does not have a name, you can specify it only by the MD level.

Examples

# Display the MA configuration information in all MDs.

```
<Sysname> display cfd ma
3 maintenance domain(s) configured.
Maintenance domain: mdtest_5
1 maintenance association(s) belong(s) to this maintenance domain:
Maintenance association: matest_5
Service instance: 5          VLAN: 5          Level: 5
```

```
Maintenance domain: mdtest_6
1 maintenance association(s) belong(s) to this maintenance domain:
Maintenance association: matest_6
Service instance: 6          VLAN: 6          Level: 6

Maintenance domain: (Without Name)
1 maintenance association(s) belong(s) to this maintenance domain:
Maintenance association: matest_7
Service instance: 7          VLAN: 7          Level: 7
```

Table 17 Command output

Field	Description
3 maintenance domain(s) configured.	Number of MDs configured
Maintenance domain	Name of the MD (if the MD does not have a name, this field is displayed as **Without Name**)
Level	MD level
1 maintenance association(s) belong(s) to this maintenance domain	Number of MAs configured in the MD
Maintenance association	Name of the MA
Service instance	Service instance of the MA
VLAN	VLAN to which the service instance belongs
Level	Level of the MD to which the MA belongs

display cfd md

Syntax

display cfd md [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd md** to display the MD configuration information.

Examples

# Display the MD configuration information.

```
<Sysname> display cfd md
CFD is enabled.
8 maintenance domain(s) configured:
Level: 0     Maintenance domain: mdtest_0
Level: 1     Maintenance domain: mdtest_1
Level: 2     Maintenance domain: mdtest_2
Level: 3     Maintenance domain: mdtest_3
Level: 4     Maintenance domain: mdtest_4
Level: 5     Maintenance domain: mdtest_5
Level: 6     Maintenance domain: mdtest_6
Level: 7     Maintenance domain: (Without Name)
```

Table 18 Command output

Field	Description
8 maintenance domain(s) configured	Number of MDs configured.
Level	Level of MD. Each level allows only one MD.
Maintenance domain	Name of MD (if the MD does not have a name, this field is displayed as **Without Name**).

display cfd mep

Syntax

display cfd mep *mep-id* **service-instance** *instance-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

mep *mep-id*: Specifies a MEP by its ID, ranging from 1 to 8191.

service-instance *instance-id*: Specifies a service instance by its ID, ranging from 1 to 32767.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd mep** to display the attribute and operating information of a MEP.

Examples

# Display the attribute and operating information of MEP 50 in service instance 1.

```
<Sysname> display cfd mep 50 service-instance 1
Interface: GigabitEthernet1/0/2
Maintenance domain: mdtest_1
Maintenance association: matest_1
Level: 1        VLAN: 1         Direction: Outbound
Administrative state: Active          CCM send: Enable
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s       SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0          ReceiveInOrderLBR: 0          ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0          ReceiveLTM: 0

No CCM from some remote MEPs is received.

One or more streams of error CCMs is received. The last-received CCM:
Maintenance domain: (Without Name)
Maintenance association:matest1
MEP:5      Sequence Number:0x50A
Received Time: 02/3/6 13:01:34

One or more streams of cross-connect CCMs is received. The last-received CCM:
Maintenance domain:mdtest1
Maintenance association:matest1
MEP:6      Sequence Number:0x63A
Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit.
```

Table 19 Command output

Field	Description
Interface	Interface that an MD belongs to.
Maintenance domain	MD that a MEP belongs to (if the MD does not have a name, this field is displayed as **Without Name**).
Maintenance association	MA to which a MEP belongs.
Level	Level of the MD.
VLAN	VLAN to which the MA belongs.

Field	Description
Direction	Direction of the MEPs.
Administrative state	State of MEP, either Active or Inactive.
CCM send	Whether the MEP sends CCM.
FNG state	State of FNG (Fault Notification Generator): • FNG_RESET • FNG_DEFECT • FNG_REPORT_DEFECT • FNG_DEFECT_REPORTED • FNG_DEFECT_CLEARING A hyphen (-) means not supported.
CCM	Information related to CCM.
Current state	State of CCMs sent: • CCI_IDLE • CCI_WAITING A hyphen (-) means not supported.
Interval	Interval to send CCM.
SendCCM	Number of CCMs that have been sent by the MEPs. A hyphen (-) means not supported.
Loopback	Information related to Loopback.
NextSeqNumber	Sequence number of the next LBM to be sent.
SendLBR	Number of LBRs that have been sent. If the MEP is inward-facing, the number of LBRs will not be counted.
ReceiveInOrderLBR	Number of LBR messages received in correct sequence.
ReceiveOutOrderLBR	Number of LBR messages received out of order.
Linktrace	Information related to linktrace.
NextSeqNumber	Sequence number of the next LTM to be sent.
SendLTR	Number of LTRs sent. If the MEP is inward-facing, the number of LTRs will not be counted.
ReceiveLTM	Number of LTMs received.
No CCM from some remote MEPs is received.	Failure to receive CCMs from some remote MEPs (This information is displayed only when some CCMs are lost.)
One or more streams of error CCMs is received. The last-received CCM:	Display the content of the last error CCM when one or more error CCMs are received. (This information is displayed only when error CCM(s) is/are received.)
Maintenance domain	MD of the last error CCM message. A hyphen (-) means not supported.
Maintenance association	MA of the last error CCM message. A hyphen (-) means not supported.
MEP	ID of the MEP that sent the last error CCM message. A hyphen (-) means not supported.

Field	Description
Sequence Number	Sequence number of the last error CCM. A hyphen (-) means not supported.
Received Time	Time when the last error CCM is received.
One or more streams of cross-connect CCMs is received. The last-received CCM:	Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCM(s) is/are received.)
Some other MEPs are transmitting the RDI bit.	CCMs with the RDI flag bits set are received from other MEPs. (This information is displayed only when this type of CCM(s) is/are received.)

display cfd meplist

Syntax

display cfd meplist [**service-instance** *instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, ranging from 1 to 32767.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd meplist** to display the MEP list in a service instance.

If the service instance ID is not specified, this command displays MEP lists in all service instances.

Examples

# Display the MEP list in service instance 5.

```
<Sysname> display cfd meplist service-instance 5
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

display cfd mp

Syntax

display cfd mp [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays MP information for the port specified by its port type and port number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd mp** to display MP information.

If no port is specified, this command displays the MP information on all ports.

The output is arranged by port name, then in the ascending VLAN ID order on the same port, and in the order of outward-facing MEPs (from low to high level), MIPs, and inward-facing MEPs (from high to low level) within the same VLAN.

Examples

# Display the MP information on all ports.

```
<Sysname> display cfd mp
Interface GigabitEthernet1/0/1   VLAN 100
MEP ID: 100      Level: 0    Service instance: 100    Direction: Outbound
Maintenance domain: mdtest0
Maintenance association: mainmd0

MEP ID: 105      Level: 5    Service instance: 105    Direction: Outbound
Maintenance domain: mdtest5
Maintenance association: mainmd5

MIP              Level: 6    Service instance: 106
Maintenance domain: mdtest6
Maintenance association: mainmd6

MEP ID: 104      Level: 4    Service instance: 104    Direction: Inbound
Maintenance domain: mdtest4
Maintenance association: mainmd4

MEP ID: 102      Level: 2    Service instance: 102    Direction: Inbound
Maintenance domain: mdtest2
Maintenance association: mainmd2
```

```
Interface GigabitEthernet1/0/4   VLAN 1
MEP ID: 9        Level: 6    Service instance: 6      Direction: Outbound
Maintenance domain: mdtest6
Maintenance association: matest6
```

Table 20 Command output

Field	Description
Interface GigabitEthernet1/0/1 VLAN 100	MP configuration of the specified VLAN on the specified port
MEP ID	ID of the MEP
MIP	A MIP in the MP
Level	MD level that an MP belongs to
Service instance	Service instance to which the MP belongs
Direction	Direction of the MEP
Maintenance domain	MD to which an MP belongs
Maintenance association	MA to which an MP belongs

display cfd remote-mep

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a remote MEP, ranging from 1 to 8191.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd remote-mep** to display information about a remote MEP.

Examples

# Display information about remote MEP 10 in service instance 4.

```
<Sysname> display cfd remote-mep service-instance 4 mep 10
```

```
MEP ID   MAC Address      State        Time                 MAC Status
20       00E0-FC00-6565   OK           2006/03/06 02:36:38  UP
30       00E0-FC27-6502   OK           2006/03/06 02:36:38  DOWN
40       00E0-FC00-6510   FAILED       2006/03/06 02:36:39  DOWN
50       00E0-FC52-BAA0   OK           2006/03/06 02:36:44  DOWN
60       0010-FC00-6502   OK           2006/03/06 02:36:42  DOWN
```

Table 21 Command output

Field	Description
MEP ID	ID of the remote MED.
MAC Address	MAC address of the remote MEP device. A hyphen (-) means not supported.
State	Running state of the remote MEP, which can be OK or FAILED.
Time	Time when the remote MEP entered the FAILED or OK state for the last time.
MAC Status	State of the port indicated by the last CCM received from the remote MEP, which can be UP or DOWN. A hyphen (-) means not supported.

display cfd service-instance

Syntax

display cfd service-instance [*instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

instance-id: Service instance ID, ranging from 1 to 32767.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd service-instance** to display the configuration information of a service instance.

Without specifying the service instance ID, the command will display the configuration information of all service instances.

Examples

# Display the configuration information of all service instances.

```
<Sysname> display cfd service-instance
2 service instance(s) configured:
Service instance 5:
Maintenance domain: mdtest_5
Maintenance association: matest_5
Level: 5        VLAN: 5        MIP rule: None        CCM interval: 1s

Service instance 6:
Maintenance domain: mdtest_6
Maintenance association: matest_6
Level: 6        VLAN: 6        MIP rule: None        CCM interval: 1s
MEP ID: 730     Interface: GigabitEthernet1/0/1                Direction: Inbound

Service instance 6:
Maintenance domain: (Without Name)
Maintenance association: matest_6
Level: 6        VLAN: 6        MIP rule: None        CCM interval: 1s
MEP ID: 731     Interface: GigabitEthernet1/0/2                Direction: Outbound
```

Table 22 Command output

Field	Description
2 service instance(s) are configured.	Number of service instance configured.
Service instance 5	Service instance ID
Maintenance domain	MD of the service instance (if the MD does not have a name, this field is displayed as **Without Name**)
Maintenance association:	MA of the service instances
Level	MD level
VLAN	VLAN that the MA belongs to
MIP rule	MIP generation rules configured on service instance
CCM interval	Interval to send CCMs
MEP ID	ID of MEPs configured on the service instance
Interface	Interface of the MEP configured on the service instance
Direction	Direction of the MEPs configured on the service instance

display cfd status

Syntax

display cfd status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd status** to display the status of CFD and AIS (enabled or disabled).

Examples

# Display the status of CFD and AIS.

```
<Sysname> display cfd status
CFD is enabled.
AIS is disabled.
```

display cfd tst

Syntax

display cfd tst [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the MEP by its ID, which ranges from 1 to 8191.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd tst** to display the TST result on the specified MEP.

If no MEP is specified, the **display cfd tst** command displays the TST results of all MEPs in the specified service instance.

If no service instance is specified, the **display cfd tst** command displays the TST results of all MEPs in all service instances.

Related commands: **cfd tst**.

Examples

# Display the TST results of all the MEPs in all service instances.

```
<Sysname> display cfd tst
Service instance: 1
MEP ID: 1003
Send TST total number: 0
Received TST total number: 5
Received from 0010-FC00-6510, sequence number 1: Bit True
Received from 0010-FC00-6510, sequence number 2: Bit True
Received from 0010-FC00-6510, sequence number 3: Bit True
Received from 0010-FC00-6510, sequence number 4: Bit True
Received from 0010-FC00-6510, sequence number 5: Bit True
MEP ID: 1004
Send TST total number: 5
Received TST total number: 0

Service instance: 2
No mep exists in the service instance.

Service instance: 3
MEP ID: 1023
Send TST total number: 5
Received TST total number: 0
```

Table 23 Command output

Field	Description
Service instance	Service instance of the MEP.
Send TST total number	Number of TST frames sent.
Received TST total number	Number of TST frames received.
Received from 0010-FC00-6510, sequence number 01	TST frame with sequence number 01 received from the MEP with MAC address 0010-FC00-6510: • **Bit True**—No bit error occurred. • **Bit False**—Bit errors occurred.

display cfd version

Syntax

display cfd version [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cfd version** to display the CFD protocol version.

Examples

# Display the CFD protocol version.

```
<Sysname> display cfd version
The current CFD version is standard.
```

Table 24 Command output

Field	Description
The current CFD version is draft5	Indicates that the current CFD protocol is IEEE 802.1ag draft5.2
The current CFD version is draft5-plus	Indicates that the current CFD protocol is the IEEE 802.1ag draft5.2 interim version
The current CFD version is standard	Indicates that the current CFD protocol is the standard version of IEEE 802.1ag

reset cfd dm one-way history

Syntax

reset cfd dm one-way history [**service-instance** *instance-id* [**mep** *mep-id*]]

View

User view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the MEP by its ID, which ranges from 1 to 8191.

Description

Use **reset cfd dm one-way history** to clear the one-way DM result on the specified MEP.

If no MEP is specified, the **reset cfd dm one-way history** command clears the one-way DM results of all MEPs in the specified service instance.

If no service instance is specified, the **reset cfd dm one-way history** command clears the one-way DM results of all MEPs in all service instances.

Related commands: **display cfd dm one-way history**.

Examples

# Clear the one-way DM results of all the MEPs in all service instances.

```
<Sysname> reset cfd dm one-way history
```

reset cfd tst

Syntax

reset cfd tst [**service-instance** *instance-id* [**mep** *mep-id*]]

View

User view

Default level

1: Monitor level

Parameters

service-instance *instance-id*: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep *mep-id*: Specifies the MEP by its ID, which ranges from 1 to 8191.

Description

Use **reset cfd tst** to clear the TST result on the specified MEP.

If no MEP is specified, the **reset cfd tst** command clear the TST results of all MEPs in the specified service instance.

If no service instance is specified, the **reset cfd tst** command clears the TST results of all MEPs in all service instances.

Related commands: **display cfd tst**.

Examples

# Clear the TST results of all the MEPs in all service instances.

```
<Sysname> reset cfd tst
```

DLDP configuration commands

display dldp

Syntax

display dldp [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies a port by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dldp** to display the DLDP configuration of a port.

If no port is specified, this command displays the DLDP configuration of all DLDP-enabled ports.

Examples

# Display the DLDP configuration of all the DLDP-enabled ports.

```
<Sysname> display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : simple, password is ******
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 2s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1 (the maximum number ever detected is 2).
         Neighbor mac address : 0000-0000-0100
         Neighbor port index : 79
         Neighbor state : two way
         Neighbor aged time : 13

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0000-0000-1100
         Neighbor port index : 81
         Neighbor state : two way
         Neighbor aged time : 12
```

# Display the DLDP configuration of GigabitEthernet 1/0/49.

```
<Sysname> display dldp gigabitethernet 1/0/49
Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0000-0000-0100
         Neighbor port index : 79
         Neighbor state : two way
         Neighbor aged time : 13
```

Table 25 Command output

Field	Description
DLDP global status	Global DLDP state (enable or disable).
DLDP interval	Interval for sending Advertisement packets (in seconds) to maintain neighbor relations.
DLDP work-mode	DLDP mode (enhance or normal).
DLDP authentication-mode	DLDP authentication mode (none, simple, or md5).
password	Password for DLDP authentication, which is displayed as asterisks (******).
DLDP unidirectional-shutdown	Port shutdown mode (auto or manual) after unidirectional links are detected.
DLDP delaydown-timer	Setting of the DelayDown timer.
The number of enabled ports	Number of the DLDP-enabled ports.
Interface	Index of a DLDP-enabled port.
DLDP port state	DLDP state on a port: • initial • inactive • active • advertisement • probe • disable • disable (loopback): The port is in disable state because it has received loopback packets. • delaydown

Field	Description
DLDP link state	Port state (up or down).
The neighbor number of the port	Current number of neighbors.
the maximum number ever detected is 2	Maximum number of neighbors once detected on the port. This field appears only when the current number of neighbors is different from the maximum number of neighbors once detected.
Neighbor mac address	MAC address of the neighbor.
Neighbor port index	Neighbor port index.
Neighbor state	Neighbor state (unknown, one way, or two way).
Neighbor aged time	Neighbor aging time.

display dldp statistics

Syntax

display dldp statistics [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies a port by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dldp statistics** to display DLDP packet statistics on thes passing through a port.

If no port is specified, this command displays DLDP packet statistics passing through all the DLDP-enabled ports.

Examples

# Display DLDP packet statistics passing through all the DLDP-enabled ports.

```
<Sysname> display dldp statistics
Interface GigabitEthernet1/0/49
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 3

Interface GigabitEthernet1/0/50
 Packets sent : 7
 Packets received : 7
 Invalid packets received : 3
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 4
```

# Display DLDP packet statistics passing through GigabitEthernet 1/0/49.

```
<Sysname> display dldp statistics gigabitethernet 1/0/49
Interface GigabitEthernet1/0/49
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 3
```

Table 26 Command output

Field	Description
Interface	Port index
Packets sent	Total number of DLDP packets sent
Packets received	Total number of DLDP packets received
Invalid packets received	Number of the invalid packets received
Loop packets received	Number of the loopback packets received
Authentication failed packets received	Number of the received packets that failed to pass the authentication
Valid packets received	Number of the valid packets received

dldp authentication-mode

Syntax

dldp authentication-mode { **none** | { **md5** | **simple** } *password* }

undo dldp authentication-mode

View

System view

Default level

2: System level

Parameters

none: Specifies not to perform authentication.

md5: Specifies the MD5 authentication mode and sets a plaintext or ciphertext password.

simple: Specifies the simple authentication mode and sets a plaintext or ciphertext password.

password: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

Description

Use **dldp authentication-mode** to configure DLDP authentication.

Use **undo dldp authentication-mode** to restore the default.

By default, DLDP authentication is not performed.

To enable DLDP to operate properly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

The DLDP authentication password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

Examples

# Configure the simple authentication mode and set the plaintext password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple abc
```

- Configure Device B

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple abc
```

dldp delaydown-timer

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

View

System view

Default level

2: System level

Parameters

time: Sets the DelayDown timer, in the range of 1 to 5 seconds.

Description

Use **dldp delaydown-timer** to set the DelayDown timer.

Use **undo dldp delaydown-timer** to restore the default.

By default, the setting of the DelayDown timer is 1 second.

The DelayDown timer configured by using this command applies to all DLDP-enabled ports.

Examples

# Set the DelayDown timer to 2 seconds.

```
<Sysname> system-view
```

```
[Sysname] dldp delaydown-timer 2
```

dldp enable

Syntax

dldp enable

undo dldp enable

View

System view, Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **dldp enable** to enable DLDP.

Use **undo dldp enable** to disable DLDP.

By default, DLDP is disabled both globally and on each port.

When executed in system view, this command takes effect globally. When executed in Layer 2 Ethernet interface view, this command takes effect on the current port. When executed in port group view, this command takes effect on all the ports in the port group.

DLDP can take effect only after you enable it globally and then on a port.

Examples

# Enable DLDP globally, and then enable DLDP on GigabitEthernet 1/0/49.

```
<Sysname> system-view
[Sysname] dldp enable
[Sysname] interface gigabitethernet 1/0/49
[Sysname-GigabitEthernet1/0/49] dldp enable
```

# Enable DLDP globally, and then enable DLDP for all the ports in port group 1.

```
<Sysname> system-view
[Sysname] dldp enable
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/49 to gigabitethernet
1/0/50
[Sysname-port-group-manual-1] dldp enable
```

dldp interval

Syntax

dldp interval *time*

undo dldp interval

View

System view

Default level

2: System level

Parameters

time: Sets the interval for sending Advertisement packets, in the range of 1 to 100 seconds.

Description

Use **dldp interval** to set the interval for sending Advertisement packets.

Use **undo dldp interval** to restore the default.

By default, the interval for sending Advertisement packets is five seconds.

This command applies to all DLDP-enabled ports.

Examples

# Set the interval for sending Advertisement packets to 20 seconds.

```
<Sysname> system-view
[Sysname] dldp interval 20
```

dldp reset

Syntax

dldp reset

View

System view, Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **dldp reset** to reset the DLDP state for ports, enabling DLDP down ports to perform unidirectional link detection.

When executed in system view, this command applies to all ports of the device. When executed in Layer 2 Ethernet interface view, this command applies to the current port. When executed in port group view, this command applies to all ports in the port group.

Related commands: **dldp enable** and **dldp unidirectional-shutdown**.

Examples

# Reset DLDP state for all ports.

```
<Sysname> system-view
[Sysname] dldp reset
```

# Reset DLDP state for port GigabitEthernet 1/0/49.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/49
[Sysname-GigabitEthernet1/0/49] dldp reset
```

# Reset DLDP state for all ports in port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/49 to gigabitethernet
1/0/50
[Sysname-port-group-manual-1] dldp reset
```

dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown

View

System view

Default level

2: System level

Parameters

auto: Configures the port shutdown mode as auto mode, where, when a unidirectional link is detected, the port involved is shut down by DLDP.

manual: Configures the port shutdown mode as manual mode, where, when a unidirectional link is detected, DLDP generates log and traps to prompt you to shut down the involved port instead of doing so automatically.

Description

Use **dldp unidirectional-shutdown** to set the port shutdown mode.

Use **undo dldp unidirectional-shutdown** to restore the default.

By default, the port shutdown mode is auto mode.

Related commands: **dldp work-mode**.

Examples

# Set the port shutdown mode to auto mode.

```
<Sysname> system-view
[Sysname] dldp unidirectional-shutdown auto
```

dldp work-mode

Syntax

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode

View

System view

Default level

2: System level

Parameters

enhance: Specifies the enhanced DLDP mode.

normal: Specifies the normal DLDP mode.

Description

Use **dldp work-mode** to set the DLDP mode.

Use **undo dldp work-mode** to restore the default DLDP mode.

By default, a device operates in normal DLDP mode.

Examples

# Configure the device to operate in enhanced DLDP mode.

```
<Sysname> system-view
[Sysname] dldp work-mode enhance
```

reset dldp statistics

Syntax

reset dldp statistics [*interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies a port by its type and number.

Description

Use **reset dldp statistics** to clear DLDP packets statistics passing through a port.

If no port is specified, this command clears the DLDP packet statistics passing through all the DLDP-enabled ports.

Examples

# Clear the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> reset dldp statistics
```

RRPP configuration commands

control-vlan

Syntax

control-vlan *vlan-id*

undo control-vlan

View

RRPP domain view

Default level

2: System level

Parameters

vlan-id: ID of the primary control VLAN for the RRPP domain, which ranges from 2 to 4093.

Description

Use **control-vlan** to configure the primary control VLAN for the current RRPP domain.

Use **undo control-vlan** to remove the control VLAN configurations for the current RRPP domain.

By default, no primary control VLAN exists in the RRPP domain.

When configuring control VLANs for an RRPP domain, you only need to configure the control VLAN for the primary ring (the primary control VLAN). The system automatically configures the VLAN whose VLAN ID is the primary control VLAN ID plus 1 as the secondary control VLAN for subrings. Like the primary control VLAN, the secondary control VLAN must be a new one (not yet created). For the control VLAN configuration to succeed, you must make sure that the IDs of the two control VLANs have not yet been assigned.

Before configuring RRPP rings for an RRPP domain, you can delete or modify the control VLANs configured for the RRPP domain. However, after configuring RRPP rings for an RRPP domain, you cannot delete or modify the control VLANs of the domain.

You cannot use the **undo vlan all** command to delete a control VLAN.

Related commands: **rrpp domain**.

Examples

# Configure VLAN 100 (a non-existent VLAN) as the primary control VLAN of RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
```

display rrpp brief

Syntax

display rrpp brief [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rrpp brief** to display the brief RRPP information.

Examples

# Display the brief RRPP information.

```
<Sysname> display rrpp brief
Flags for Node Mode :
M –- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains: 2

Domain ID     : 1
Control VLAN  : Major 5    Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer   : 1  sec  Fail Timer : 3  sec
 Ring  Ring   Node  Primary/Common             Secondary/Edge             Enable
 ID    Level  Mode  Port                       Port                       Status
--------------------------------------------------------------------------------
 1     1      M     GE1/0/1                    GE1/0/2                    Yes

Domain ID     : 2
Control VLAN  : Major 10    Sub 11
Hello Timer   : 1  sec  Fail Timer : 3  sec
Protected VLAN: Reference Instance 0 to 2, 4
 Ring  Ring   Node  Primary/Common             Secondary/Edge             Enable
 ID    Level  Mode  Port                       Port                       Status
--------------------------------------------------------------------------------
 1     0      T     GE1/0/3                    GE1/0/4                    Yes
 2     1      E     GE1/0/3                    GE1/0/5                    Yes
                    GE1/0/4
```

Table 27 Command output

Field	Description
Flags for Node Mode	RRPP node mode: - M represents master node. - T represents transit node. - E represents edge node. - A represents assistant edge node.
RRPP Protocol Status	RRPP protocol status: - Enable (globally enabled) - Disable (globally disabled)
Number of RRPP Domains	Number of RRPP domains configured.
Domain ID	RRPP domain ID.
Control VLAN	Control VLANs of the RRPP domain: Major and Sub.
Protected VLAN	List of VLANs protected by the RRPP domain. Multiple Spanning Tree Instances (MSTIs) are displayed here. To get the VLANs corresponding to these MSTIs, use the **display stp region-configuration** command.
Hello Timer	Hello Timer value in seconds.
Fail Timer	Fail Timer value in seconds.
Ring ID	RRPP ring ID.
Ring Level	RRPP ring level - 0 representing primary ring. - 1 representing subring.
Node Mode	Node mode.
Primary/Common Port	- Primary port when the node mode is master node or transit node. - Common port when the node mode is edge node or assistant edge node. - A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Secondary/Edge Port	- Secondary port when the node mode is master node or transit node. - Edge port when the node mode is edge node or assistant edge node. - A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Enable Status	RRPP ring status: - Yes indicates enabled. - No indicates disabled.

display rrpp ring-group

Syntax

display rrpp ring-group [*ring-group-id*] [**\|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor Level

Parameters

ring-group-id: RRPP ring group ID, which ranges from 1 to 8.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rrpp ring-group** to display the RRPP ring group configuration.

If no ring group ID is specified, this command displays the configuration of all ring groups.

If an RRPP ring ID is specified, this command displays the configuration of the specified RRPP ring group on the current device.

For an edge node RRPP ring group, this command also displays the subring sending Edge-Hello packets.

Related commands: **domain ring**.

Examples

# Display the configuration of all RRPP ring groups.

```
<Sysname> display rrpp ring-group
Ring Group 1:
domain 1 ring 1 to 3, 5
domain 2 ring 1 to 3, 5
domain 1 ring 1 is the sending ring

Ring Group 2:
domain 1 ring 4, 6 to 7
domain 2 ring 4, 6 to 7
```

Table 28 Command output

Field	Description
Ring Group 1	RRPP ring group 1.
domain 1 ring 1 to 3, 5	Subrings in the ring group, including rings 1, 2, 3, and 5 in RRPP domain 1.
domain 1 ring 1 is the sending ring	The sending ring of the ring group is ring 1 in RRPP domain 1.

display rrpp statistics

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

domain-id: RRPP domain ID, which ranges from 1 to 8.

ring-id: RRPP ring ID, which ranges from 1 to 64.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rrpp statistics** to display RRPPDU statistics.

If an RRPP ring ID is specified, this command displays RRPPDU statistics for the specified RRPP ring in the specified RRPP domain. If not, this command displays RRPPDU statistics for all RRPP rings in the specified RRPP domain.

If a port belongs to more than one ring, this command collects and displays its RRPPDU statistics by ring.

When a ring transits from inactive to active, packet counting for the ring restarts.

Related commands: **reset rrpp statistics**.

Examples

# Display the RRPPDU statistics for ring 1 in RRPP domain 1.

```
<Sysname> display rrpp statistics domain 1 ring 1
Ring ID       : 1
Ring Level    : 1
Node Mode     : Master
Active Status : Yes
Primary port  : GE1/0/1
 Packet           Link      Common     Complete   Edge      Major     Packet
 Direct Hello     Down      Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   16424     0         0          1          0         0         16425
 Rcv    0         0         0          0          0         0         0
Secondary port: GE1/0/2
 Packet           Link      Common     Complete   Edge      Major     Packet
 Direct Hello     Down      Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   0         0         0          0          0         0         0
 Rcv    16378     0         0          1          0         0         16379
```

# Display the RRPPDU statistics for all rings in RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
```

```
Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Active Status : Yes
Primary port  : GE1/0/3
 Packet           Link     Common     Complete   Edge      Major     Packet
 Direct Hello     Down     Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   16924     0        0          1          0         0         16925
 Rcv    0         0        0          0          0         0         0
Secondary port: GE1/0/4
 Packet           Link     Common     Complete   Edge      Major     Packet
 Direct Hello     Down     Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   0         0        0          0          0         0         0
 Rcv    16878     0        0          1          0         0         16879

Ring ID        : 2
Ring Level     : 1
Node Mode      : Edge
Active Status : No
Common port    : GE1/0/3
 Packet           Link     Common     Complete   Edge      Major     Packet
 Direct Hello     Down     Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   0         0        0          0          0         0         0
 Rcv    0         0        0          0          0         0         0
Common port    : GE1/0/4
 Packet           Link     Common     Complete   Edge      Major     Packet
 Direct Hello     Down     Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   0         0        0          0          0         0         0
 Rcv    0         0        0          0          0         0         0
Edge port      : GE1/0/5
 Packet           Link     Common     Complete   Edge      Major     Packet
 Direct Hello     Down     Flush FDB  Flush FDB  Hello     Fault     Total
------------------------------------------------------------------------------
 Send   0         0        0          0          0         0         0
 Rcv    0         0        0          0          0         0         0
```

Table 29 Command output

Field	Description
Ring ID	RRPP ring ID.
Ring Level	RRPP ring level: • 0 for primary ring. • 1 for subring.

Field	Description
Node Mode	Node mode: - Master node. - Transit node. - Edge node. - Assistant edge node.
Active Status	RRPP ring activation status: - Yes for active. - No for inactive.
Primary Port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Secondary Port	The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Common Port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Packet Direct	Packet transmission direction on the port: Send or Rcv.
Hello	Hello packet statistics received/sent on the port.
Link Down	Link-Down packet statistics received/sent on the port.
Common Flush FDB	Common-Flush-FDB packet statistics received/sent on the port.
Complete Flush FDB	Complete-Flush-FDB packet statistics received/sent on the port.
Edge Hello	Edge-Hello packet statistics received/sent on the port.
Major Fault	Major-Fault packet statistics received/sent on the port.
Packet Total	Total number of packets received/sent on the port. Here only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted.

display rrpp verbose

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

domain-id: RRPP domain ID, which ranges from 1 to 8.

ring-id: RRPP ring ID, which ranges from 1 to 64.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rrpp verbose** to display detailed RRPP information.

If an RRPP ring ID is specified, this command displays the detailed information of the specified ring in the specified RRPP domain. Otherwise, this command displays the detailed information of all the rings in the specified RRPP domain.

Examples

# Display the detailed information of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 5    Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer    : 1  sec  Fail Timer : 3  sec
Ring ID        : 1
Ring Level     : 1
Node Mode      : Master
Ring State     : Complete
Enable Status : Yes    Active Status: Yes
Primary port   : GE1/0/1                     Port status: UP
Secondary port: GE1/0/2                      Port status: BLOCKED
```

# Display the detailed information of all the rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
Domain ID      : 2
Control VLAN   : Major 10    Sub 11
Protected VLAN: Reference Instance 3, 5 to 7
Hello Timer    : 1  sec  Fail Timer : 3  sec

Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Enable Status : Yes    Active Status: Yes
Primary port   : GE1/0/4                     Port status: UP
Secondary port: GE1/0/5                      Port status: BLOCKED

Ring ID        : 2
Ring Level     : 1
Node Mode      : Edge
Ring State     : -
```

```
Enable Status : No    Active Status: No
Common port   : GE1/0/4                     Port status: -
                GE1/0/5                     Port status: -
Edge port     : GE1/0/3                     Port status: -
```

Table 30 Command output

Field	Description
Domain ID	RRPP domain ID.
Control VLAN	Control VLANs of the RRPP domain: • **Major**—Represents the primary control VLAN. • **Sub**—Represents the secondary control VLAN.
Protected VLAN	List of VLANs protected by the RRPP domain. MSTIs are displayed here. To get the VLANs corresponding to these MSTIs, use the **display stp region-configuration** command.
Hello Timer	Hello Timer value in seconds.
Fail Timer	Fail Timer value in seconds.
Ring ID	RRPP ring ID.
Ring Level	RRPP ring level: • 0 representing primary ring. • 1 representing subring.
Node Mode	Node mode: • Master node. • Transit node. • Edge node. • Assistant edge node.
Ring State	RRPP ring state: • **Complete**—The ring is healthy. • **Failed**—The ring is not closed. • If the ring is not enabled on the device working as the master node or the device is not the master node of the ring, a hyphen (-) is displayed.
Enable Status	RRPP ring enable status: • Yes for enabled. • No for disabled.
Active Status	RRPP ring activation status. An RRPP ring can be active only when the RRPP protocol and the RRPP ring are both enabled. You can also use this field to identify whether the RRPP protocol are enabled. Two statuses are available: • Yes for active. • No for inactive.
Primary Port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Secondary Port	The secondary port field means the node mode is master node or transit node. **-** appears when the port is not configured on the ring or the board to which the port belongs does not start.

Field	Description
Common Port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when the port is not configured on the ring or the board to which the port belongs does not start.
Port status	Port status includes down, up and blocked; a hyphen (-) appears in one of the following cases: • The ring is inactive. • The port is not configured on the ring. • The board to which the port belongs does not start.

domain ring

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

View

RRPP ring group view

Default level

2: System level

Parameters

domain-id: RRPP domain ID, which ranges from 1 to 8.

ring-id-list: RRPP subring ID list expressed in the format of *ring-id-list*={ *ring-id* [**to** *ring-id*] }&<1-10>, where the *ring-id* argument is an RRPP subring ID in the range of 1 to 64 and &<1-10> indicates that you can input up to ten RRPP ring ID ranges.

Description

Use **domain ring** to configure subrings for an RRPP ring group.

Use **undo domain ring** to remove the specified subring(s) from an RRPP ring group. If no subring ID list is specified, all subrings in the ring group are removed in the specified domain.

Follow these guidelines when configuring an RRPP ring group on the edge node and the assistant-edge node:

- When assigning an active ring to a ring group, do that on the assistant-edge node first and then on the edge node.
- To remove an active ring from a ring group, do that on the edge node first and then on the assistant-edge node.
- To remove the whole ring group, do that on the edge node first and then on the assistant-edge node.
- When activating rings in a ring group, do that on the assistant-edge node first and then on the edge node.
- When deactivating rings in a ring group, do that on the edge node first and then on the assistant-edge node.

Failure to follow these guidelines can cause the failure of assistant-edge node to receive Edge-Hello packets and mistakenly considering the primary ring as failed.

Related commands: **rrpp ring-group** and **display rrpp ring-group**.

Examples

# Configure subrings for RRPP ring group 1.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1] domain 1 ring 1 to 3 5
[Sysname-rrpp-ring-group1] domain 2 ring 1 to 3 5
```

protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

View

RRPP domain view

Default level

2: System level

Parameters

reference-instance *instance-id-list*: Specifies the MSTIs you want to reference in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>. The *instance-id* argument is an MSTI ID that ranges from 0 to 32. *&<1-10>* means that you can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the instance-to-VLAN mappings (a device working in PVST mode automatically maps VLANs to MSTIs).

Description

Use **protected-vlan** to configure the protected VLANs for the RRPP domain. The protected VLANs are specified by the MSTIs.

Use **undo protected-vlan** to remove the specified protected VLANs of the RRPP domain. If no MSTI is specified, all protected VLANs of the RRPP domain are removed.

By default, no protected VLAN is specified for an RRPP domain.

To be compatible with old-version RRPP, which does not support protected VLAN configuration, an RRPP domain protects all VLANs on a device started with an old-version configuration file.

You can delete or modify the protected VLANs configured for an RRPP domain before and after configuring rings for it. However, you cannot delete all the protected VLANs configured for the domain.

When the VLAN-to-MSTI mappings change, the protected VLANs of an RRPP domain also changes according to the MSTIs configured for the domain.

Related commands: **rrpp domain**; **display stp region-configuration** (*Layer 2—LAN Switching Command Reference*).

Examples

# Map VLANs 1 through 30 to MSTI 1, activate the MST region configuration, configure VLAN 100 as the control VLAN of RRPP domain 1, and configure VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 1
```

reset rrpp statistics

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

User view

Default level

1: Monitor level

Parameters

domain-id: RRPP domain ID, which ranges from 1 to 8.

ring-id: RRPP ring ID, which ranges from 1 to 64.

Description

Use **reset rrpp statistics** to clear RRPPDU statistics.

If an RRPP ring ID is specified, this command clears the RRPPDU statistics for the specified RRPP ring in the specified RRPP domain. Otherwise, this command clears the RRPPDU statistics for all RRPP rings in the specified RRPP domain.

Related commands: **display rrpp statistics**.

Examples

# Clear the RRPPDU statistics for ring 10 in RRPP domain 1.

```
<Sysname> reset rrpp statistics domain 1 ring 10
```

ring

Syntax

ring *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **edge** | **assistant-edge** } [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

View

RRPP domain view

Default level

2: System level

Parameters

ring-id: RRPP ring ID, which ranges from 1 to 64.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

interface-type interface-number: Specifies a port by its type and number. The port can be a Layer-2 Ethernet port or Layer-2 aggregate interface.

secondary-port: Specifies the port as a secondary port.

level-value: RRPP ring level, with 0 representing primary ring and 1 representing subring.

edge: Specifies the device as the edge node of the RRPP ring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

edge-port: Specifies the edge port for the node.

Description

Use **ring** to configure the node mode of the device, the role of the specified RRPP port, and the level of the RRPP ring.

Use **undo ring** to remove the configuration.

The ID of an RRPP ring in a domain must be unique.

When an RRPP is enabled, you cannot configure its RRPP ports.

When configuring the edge node and the assistant-edge node, first configure the primary ring, and then the subrings.

The node mode, RRPP port role, and ring level settings of an RRPP ring cannot be modified once they are configured. To modify the settings, first remove the present settings.

You must remove all subring configurations before deleting the primary ring configuration of the edge node or the assistant-edge node. However, an active RRPP ring cannot be deleted.

Related command: **ring enable**.

Examples

# Specify the device as the master node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

# Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
```

```
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

# Specify the device as the master node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

# Specify the device as the transit node of primary ring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

# Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Then, specify the device as the edge node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/3
```

# Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Then, specify the device as the assistant edge node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

ring enable

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

View

RRPP domain view

Default level

2: System level

Parameters

ring-id: RRPP ring ID, which ranges from 1 to 64.

Description

Use **ring enable** to enable the RRPP ring.

Use **undo ring enable** to disable the RRPP ring.

By default, the RRPP ring is disabled.

To activate the RRPP domain, enable the RRPP protocol and the RRPP rings for the RRPP domain.

Related commands: **rrpp enable**.

Examples

# Enable RRPP ring 10 in RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 10 enable
```

rrpp domain

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

View

System view

Default level

2: System level

Parameters

domain-id: RRPP domain ID, which ranges from 1 to 8.

Description

Use **rrpp domain** to create an RRPP domain and enter its view.

Use **undo rrpp domain** to remove an RRPP domain.

When you delete an RRPP domain, its control VLANs are deleted, and its protected VLAN configuration is deleted at the same time.

To delete an RRPP domain successfully, make sure it has no RRPP rings.

Related commands: **control-vlan** and **protected-vlan**.

Examples

# Create RRPP domain 1, and enter RRPP domain 1 view.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1]
```

rrpp enable

Syntax

rrpp enable

undo rrpp enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **rrpp enable** to enable RRPP protocol.

Use **undo rrpp enable** to disable RRPP protocol.

By default, RRPP protocol is disabled.

To activate the RRPP domain, enable the RRPP protocol and the RRPP rings for the RRPP domain.

Related commands: **ring enable**.

Examples

# Enable the RRPP protocol.

```
<Sysname> system-view
[Sysname] rrpp enable
```

rrpp ring-group

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

View

System view

Default level

2: System level

Parameters

ring-group-id: RRPP ring group ID, which ranges from 1 to 8.

Description

Use **rrpp ring-group** to create an RRPP ring group and enter RRPP ring group view.

Use **undo rrpp ring-group** to delete an RRPP ring group.

RRPP configured with ring groups cannot interoperate with RRPP that does not support ring group configuration.

When removing a ring group, do that on the edge node first and then on the assistant-edge node. If you fail to follow the order, the assistant-edge node may fail to receive Edge-Hello packets and mistakenly considers that the primary ring has failed.

After a ring group is removed, all subrings in the ring group do not belong to any ring group.

Related commands: **domain ring** and **display rrpp ring-group**.

Examples

# Create RRPP ring group 1 and enter its view.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1]
```

timer

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

View

RRPP domain view

Default level

2: System level

Parameters

hello-value: Hello timer value, which ranges from 1 to 10 seconds.

fail-value: Fail timer value, which ranges from 3 to 30 seconds.

Description

Use **timer** to configure the Hello timer value and the Fail timer value for the RRPP domain.

Use **undo timer** to restore it to the default value.

By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds.

The Fail timer value must be greater than or equal to three times the Hello timer value.

Examples

# Set the Hello timer value to 2 seconds and the Fail timer value to 7 seconds.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

Smart Link configuration commands

display smart-link flush

Syntax

display smart-link flush [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display smart-link flush** to display information about received flush messages.

Examples

# Display information about received flush messages.

```
<Sysname> display smart-link flush
 Received flush packets                             : 10
 Receiving interface of the last flush packet       : GigabitEthernet1/0/1
 Receiving time of the last flush packet            : 19:19:03 2010/04/21
 Device ID of the last flush packet                 : 000f-e200-8500
 Control VLAN of the last flush packet              : 1
```

Table 31 Command output

Field	Description
Received flush packets	Total number of received flush messages
Receiving interface of the last flush packet	Port that received the last flush message
Receiving time of the last flush packet	Time when the last flush message was received
Device ID of the last flush packet	Device ID carried in the last flush message
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message

display smart-link group

Syntax

display smart-link group { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Smart link group ID, which ranges from 1 to 26.

all: Displays information about all smart link groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display smart-link group** to display information about the specified or all smart link groups.

Examples

# Display information about smart link group 1.

```
<Sysname> display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e200-8500
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 1
 Protected VLAN: Reference Instance 0 to 2, 4
 Member                     Role    State    Flush-count Last-flush-time
 -----------------------------------------------------------------------------
 GigabitEthernet1/0/1       MASTER  ACTVIE   1           16:37:20 2010/04/21
 GigabitEthernet1/0/2       SLAVE   STANDBY  2           17:45:20 2010/04/21
```

Table 32 Command output

Field	Description
Smart link group 1 information	Information about smart link group 1.
Preemption mode	Preemption mode, which can be **role** for preemption enabled or **none** for preemption disabled.
Preemption delay	Preemption delay time, in seconds.
Control-VLAN	Control VLAN ID.

Field	Description
Protected VLAN	Protected VLANs of the smart link group. Referenced Multiple Spanning Tree Instances (MSTIs) are displayed here. To view the VLANs mapped to the referenced MSTIs, use the **display stp region-configuration** command.
Member	Member port of the smart link group.
Role	Port role: master or slave.
State	Port state: active, standby, or down.
Flush-count	Number of transmitted flush messages.
Last-flush-time	Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted).

flush enable

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

View

Smart link group view

Default level

2: System level

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument represents the control VLAN ID, which ranges from 1 to 4094.

Description

Use **flush enable** to enable flush update.

Use **undo flush enable** to disable flush update.

By default, flush update is enabled for smart link groups and VLAN 1 is used for flush message transmission.

Configure different control VLANs for different smart link groups.

Related commands: **smart-link flush enable**.

Examples

# Disable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] undo flush enable
```

port

Syntax

port *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number*

View

Smart link group view

Default level

2: System level

Parameters

interface-type interface-number: Specifies a port by its type and number.

master: Specifies a port as the master port.

slave: Specifies a port as the slave port.

Description

Use **port** to configure the specified port as the master or slave port of the current smart link group.

Use **undo port** to remove the specified port from the smart link group.

Disable the spanning tree feature and RRPP on the ports you want to add to the smart link group, and make sure the ports are not member ports of any aggregation group. On the other hand, you cannot enable the spanning tree feature or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group.

You can assign a port to a smart link group with the **port smart-link group** command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

Related commands: **port smart-link group**.

Examples

# Configure GigabitEthernet 1/0/1 as the slave port of smart link group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port gigabitethernet 1/0/1 slave
```

port smart-link group

Syntax

port smart-link group *group-id* { **master** | **slave** }

undo port smart-link group *group-id*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

group-id: Smart link group ID, which ranges from 1 to 26.

master: Specifies the port as the master port.

slave: Specifies the port as the slave port.

Description

Use **port smart-link group** to configure the current port as a member of the specified smart link group.

Use **undo port smart-link group** to remove the port from the specified smart link group.

Disable the spanning tree feature and RRPP on the ports you want to add to the smart link group, and make sure the ports are not member ports of any aggregation group. On the other hand, you cannot enable the spanning tree feature or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group.

You can assign a port to a smart link group with the port command in smart link group view.

Related commands: **port**.

Examples

# Configure GigabitEthernet 1/0/1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 master
```

# Configure Layer 2 aggregate interface 1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 master
```

port smart-link group track

Syntax

port smart-link group *group-id* **track cfd cc**

undo port smart-link group *group-id* **track cfd cc**

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

group-id: Number of a smart link group, which ranges from 1 to 26.

Description

Use **port smart-link group track** to configure the collaboration between a smart link group member port and the CC function of CFD.

Use **undo port smart-link group track** to remove the collaboration.

By default, smart link group member ports do not collaborate with the CC function of CFD.

Before configuring the collaboration between a port and the CC function of CFD, make sure the port is already a member port of a smart link group.

The control VLAN of the smart link group to which the port belongs must match the detection VLAN of the CC function of CFD.

Examples

# Configure the collaboration between GigabitEthernet 1/0/1, the master port of smart link group 1, and the CC function of CFD to detect the link status.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 master
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
```

preemption delay

Syntax

preemption delay *delay-time*

undo preemption delay

View

Smart link group view

Default level

2: System level

Parameters

delay-time: Preemption delay (in seconds), in the range of 0 to 300.

Description

Use **preemption delay** to set the preemption delay. When role preemption is enabled, after the preemption delay is set, the master port waits for a specific period before taking over to collaborate with the switchover of upstream devices.

Use **undo preemption delay** to restore the default.

By default, the preemption delay is 1 second.

The preemption delay configuration takes effect only after role preemption is enabled.

Related commands: **preemption mode**.

Examples

# Enable role preemption and set the preemption delay to 10 seconds.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

preemption mode

Syntax

preemption mode role

undo preemption mode

View

Smart link group view

Default level

2: System level

Parameters

role: Configures the role preemption mode, which enables the master port to preempt the slave port in active state.

Description

Use **preemption mode** to enable role preemption.

Use **undo preemption mode** to disable role preemption.

By default, the device is operating in non-preemption mode.

Examples

# Enable the role preemption mode.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
```

protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

View

Smart link group view

Default level

2: System level

Parameters

reference-instance *instance-id-list*: Specifies the MSTIs you want to reference in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>. The *instance-id* argument is an MSTI ID that ranges from 0 to

32. A value of 0 represents the common internal spanning tree (CIST). *&<1-10>* means that you can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the instance-to-VLAN mappings (a device working in PVST mode automatically maps VLANs to MSTIs).

Description

Use **protected-vlan** to configure protected VLANs for a smart link group by referencing MSTIs. You can use the **display stp region-configuration** command to view the VLANs mapped to the referenced MSTIs.

Use **undo protected-vlan** to remove the specified protected VLANs from a smart link group by referencing the specified MSTIs. If no MSTI is specified, all the protected VLANs of the smart link group are removed.

By default, no protected VLAN is configured for a smart link group.

Before assigning ports to a smart link group, configure protected VLANs for the smart link group.

You can remove all protected VLANs from a smart link group when the group is empty but not after a member port is assigned to it.

Removing a smart link group also removes its protected VLAN configuration.

If the VLANs mapped to a referenced MSTI change, the protected VLANs also change.

The VLANs to which the member ports of a smart link group belong must be configured as the protected VLANs of the smart link group.

Related commands: **smart-link group**; **display stp region-configuration** (*Layer 2—LAN Switching Command Reference*).

Examples

# Map VLANs 1 through 30 to MSTI 1, activate the MST region configuration, and configure the VLANs mapped to MSTI 1 as the protected VLANs of smart link group 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1
```

reset smart-link statistics

Syntax

reset smart-link statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset smart-link statistics** to clear flush message statistics.

Examples

# Clear flush message statistics.

```
<Sysname> reset smart-link statistics
```

smart-link flush enable

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

control-vlan *vlan-id-list*: Specifies the control VLANs used for receiving flush messages. The *vlan-id-list* is expressed in the form of *vlan-id-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the ID of a control VLAN and ranges from 1 to 4094. &<1-10> indicates that you can provide up to ten VLAN IDs or VLAN ID lists.

Description

Use **smart-link flush enable** to configure a receive control VLAN—a VLAN for receiving flush messages.

Use **undo smart-link flush enable** to disable flush message processing.

By default, flush messages are not processed.

If no VLAN is specified, VLAN 1 applies.

Do not use this command on the member port of an aggregation group.

Related commands: **flush enable**.

Examples

# Enable GigabitEthernet 1/0/1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] smart-link flush enable
```

# Enable Layer 2 aggregate interface 1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

smart-link group

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

View

System view

Default level

2: System level

Parameters

group-id: Smart link group ID, which ranges from 1 to 26.

Description

Use **smart-link group** to create a smart link group and enter smart link group view.

Use **undo smart-link group** to remove a smart link group.

You cannot remove a smart link group with member ports.

Examples

# Create smart link group 1 and enter smart link group view.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1]
```

Monitor Link configuration commands

display monitor-link group

Syntax

display monitor-link group { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Monitor link group ID, which ranges from 1 to 16.

all: Displays information about all monitor link groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display monitor-link group** to display monitor link group information.

Examples

# Display information about monitor link group 1.

```
<Sysname> display monitor-link group 1
 Monitor link group 1 information:
 Group status: DOWN
 Last-up-time: 16:37:20 2009/4/21
 Last-down-time: 16:38:26 2009/4/21
 Member                    Role     Status
 ------------------------------------------
 GigabitEthernet1/0/1      UPLINK   DOWN
 GigabitEthernet1/0/2      DOWNLINK DOWN
```

Table 33 Command output

Field	Description
Monitor link group 1 information	Information about monitor link group 1
Group status	Monitor link group state, which can be up or down
Last-up-time	Last time when the monitor link group was up

Field	Description
Last-down-time	Last time when the monitor link group was down
Member	Member ports of the monitor link group
Role	Port role, which can be uplink port or downlink port
Status	Member link state, which can be up or down

monitor-link group

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

View

System view

Default level

2: System level

Parameters

group-id: Monitor link group ID, which ranges from 1 to 16.

Description

Use **monitor-link group** to create a monitor link group and enter monitor link group view. If the specified monitor link group already exists, this command directly leads you to monitor link group view.

Use **undo monitor-link group** to remove a monitor link group.

Related commands: **port monitor-link group** and **port**.

Examples

# Create monitor link group 1 and enter the view of monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1]
```

port

Syntax

port *interface-type interface-number* { **uplink** | **downlink** }

undo port *interface-type interface-number*

View

Monitor link group view

Default level

2: System level

Parameters

interface-type interface-number: Specifies a port by type and number.

uplink: Specifies an uplink port.

downlink: Specifies a downlink port.

Description

Use **port** to assign a port to the monitor link group.

Use **undo port** to remove a port from the monitor link group.

You can assign Layer 2 Ethernet ports or Layer 2 aggregate interfaces to a monitor link group as member ports.

A port can be assigned to only one monitor link group.

Alternatively, you can assign a port to a monitor link group by using the **port monitor-link group** command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

Related commands: **port monitor-link group**.

Examples

# Create monitor link group 1, and configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

port monitor-link group

Syntax

port monitor-link group *group-id* { **uplink** | **downlink** }

undo port monitor-link group *group-id*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

group-id: Monitor link group ID, which ranges from 1 to 16.

uplink: Specifies an uplink port.

downlink: Specifies a downlink port.

Description

Use **port monitor-link group** to assign the current port to a monitor link group as a member port.

Use **undo port monitor-link group** to remove the current port from a monitor link group.

A port can be assigned to only one monitor link group.

Alternatively, you can assign a port to a monitor link group with the **port** command in monitor link group view.

Related commands: **port**.

Examples

# Create monitor link group 1, and configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port monitor-link group 1 downlink
```

Track configuration commands

display track

Syntax

display track { *track-entry-number* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

track-entry-number: Displays information about the specified track entry, in the range of 1 to 1024.

all: Displays information about all the track entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display track** to display track entry information.

Examples

# Display information about all track entries.

```
<Sysname> display track all
Track ID: 1
  Status: Positive (notify 13 seconds later)
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 10
Track ID: 2
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Reference object:
    Track interface  :
    Interface status : Inserted
    Interface        : Vlan-interface3
    Protocol         : IPv4
```

Table 34 Command output

Field	Description
Track ID	ID of a track entry.
Status	Status of a track entry: • **Positive**—The tracked object functions normally. • **Invalid**—The tracked object is invalid. • **Negative**—The tracked object is abnormal.
notify 13 seconds later	The track module notifies the application modules of the track entry state change 13 seconds later. The information is not displayed after the track module notifies the application modules.
Duration	Time period during which the track entry stays in the state.
Notification delay: Positive 20, Negative 30 (in seconds)	• The track module notifies the application modules that the status of the track entry changes to Positive after a delay time of 20 seconds. • The track module notifies the application modules that the status of the track entry changes to Negative after a delay time of 30 seconds.
Reference object	Tracked object associated with the track entry.
NQA entry	NQA test group associated with the track entry.
Reaction	Reaction entry associated with the track entry.
Track interface	Information of the interface associated with the track entry.
Interface status	Interface status: • Inserted • Removed
Interface	Interface to be monitored.
Protocol	Physical status or Layer 3 protocol status of the monitored interface: • **None**—Physical status of the monitored interface. • **IPv4**—IPv4 protocol status of the monitored Layer 3 interface. • **IPv6**—IPv6 protocol status of the monitored Layer 3 interface.

track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

View

System view

Default level

2: System level

Parameters

track-entry-number: Specifies a track entry ID, in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

delay: Specifies that the track module notifies the application modules of the track entry status change after a specific delay time. If this keyword is not provided, the track module notifies the application modules immediately when the track entry status changes.

negative *negative-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Negative. *negative-time* represents the delay time in seconds, in the range of 1 to 300.

positive *positive-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Positive. *positive-time* represents the delay time in seconds, in the range of 1 to 300.

Description

Use **track interface** to create a track entry, associate it with the physical status of a specific interface, and specify the delay time for the track module to notify the application modules when the status of the track entry changes.

Use **undo track** to remove the track entry.

By default, no track entry to be associated with the physical status of a specific interface is created.

After a track entry is created, you cannot change its settings except the delay time. To change the delay time, use the **track interface delay** command. To modify other settings of this track entry, first delete the entire track entry, and then create a new track entry.

When a track entry to be associated with the physical status of a specific interface is created, the status of the track entry is Positive if the physical status of the interface is up. The status of the track entry is Negative if the physical status of the interface is down. To display the physical status of an interface, use the **display ip interface brief** command.

Related commands: **display track**; **display ip interface brief** (*Layer 3—IP Services Command Reference*).

Examples

# Create track entry 1, and associate it with the physical status of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] track 1 interface gigabitethernet 1/0/1
```

track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

View

System view

Default level

2: System level

Parameters

track-entry-number: Specifies a track entry ID, in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

ipv4: Monitors the IPv4 protocol status. When the IPv4 protocol status of an interface is up, the status of the track object is Positive. When the IPv4 protocol status of an interface is down, the status of the track object is Negative. To display the IPv4 protocol status of an interface, use the **display ip interface brief** command.

ipv6: Monitors the IPv6 protocol status. When the IPv6 protocol status of an interface is up, the status of the track object is Positive. When the IPv6 protocol status of an interface is down, the status of the track object is Negative. To display the IPv6 protocol status of an interface, use the **display ipv6 interface** command.

delay: Specifies that the track module notifies the application modules of the track entry status change after a specific delay time. If this keyword is not provided, the track module notifies the application modules immediately when the track entry status changes.

negative *negative-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Negative. *negative-time* represents the delay time in seconds, in the range of 1 to 300.

positive *positive-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Positive. *positive-time* represents the delay time in seconds, in the range of 1 to 300.

Description

Use **track interface protocol** to create a track entry, associate it with the protocol status of a specific interface, and specify the delay time for the track module to notify the application modules when the status of the track entry changes.

Use **undo track** to remove the track entry.

By default, no track entry exists.

After a track entry is created, you cannot change its settings except the delay time. To change the delay time, use the **track interface protocol delay** command. To modify other settings of this track entry, first delete the entire track entry, and then create a new track entry.

Related commands: **display track**; **display ip interface brief** (*Layer 3—IP Services Command Reference)*; **display ipv6 interface** (*Layer 3—IP Services Command Reference).*

Examples

# Create track entry 1, and associate it with the IPv4 protocol status of VLAN-interface 2.

```
<Sysname> system-view
[Sysname] track 1 interface vlan-interface 2 protocol ipv4
```

track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

View

System view

Default level

2: System level

Parameters

track-entry-number: Specifies a track entry ID, in the range of 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA test group to be associated with the track entry. *admin-name* is the name of the NQA test group administrator who creates the NQA operation, and is a case-insensitive string of 1 to 32 characters. *operation-tag* is the NQA operation tag, a case-insensitive string of 1 to 32 characters.

reaction *item-number*: Specifies the reaction entry to be associated with the track entry. *item-number* is the reaction entry ID, in the range of 1 to 10.

delay: Specifies that the track module notifies the application modules of the track entry status change after a specific delay time. If this keyword is not provided, the track module notifies the application modules immediately when the track entry status changes.

negative *negative-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Negative. *negative-time* represents the delay time in seconds, in the range of 1 to 300.

positive *positive-time*: Specifies the delay time for the track module to notify the application modules that the status of the track entry changes to Positive. *positive-time* represents the delay time in seconds, in the range of 1 to 300.

Description

Use **track nqa** to create a track entry, associate it with the specified reaction entry of the NQA test group, and specify the delay time for the track module to notify the application modules when the status of the track entry changes.

Use **undo track** to remove the track entry.

By default, no track entry exists.

After a track entry is created, you cannot change its settings except the delay time. To change the delay time, use the **track nqa delay** command. To modify other settings of this track entry, first delete the entire track entry, and then create a new track entry.

Related commands: **display track**; **nqa** and **reaction** (*Network Management and Monitoring Command Reference*).

Examples

# Create track entry 1, and associate it with reaction entry 3 of the NQA test group (admin-test).

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
```

Index

Contents

Ping, tracert, and system debugging commands

Ping and tracert commands

ping

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host*

View

Any view

Default level

0: Visit level

Parameters

ip: Specifies supports of the IPv4 protocol. If this keyword is not specified, IPv4 is also supported.

-a *source-ip*: Specifies the source IP address of an ICMP echo request (ECHO-REQUEST). It must be an IP address configured on the device. If this option is not specified, the source IP address of an ICMP echo request is the primary IP address of the outbound interface of the request.

-c *count*: Specifies the number of times that an ICMP echo request is sent, which is in the range of 1 to 4294967295 and defaults to 5.

-f: Discards packets larger than the MTU of a given interface, which means the ICMP echo request is not allowed to be fragmented.

-h *ttl*: Specifies the TTL value for an ICMP echo request, which is in the range of 1 to 255 and defaults to 255.

-i *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number. If this option is not specified, the ICMP echo request sending interface is determined by searching the routing table or forwarding table according to the destination IP address.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMP echo request, which is in the range of 1 to 65535 and defaults to 200.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-n: Disables domain name resolution for the *host* argument. When this keyword is not specified, if the host argument represents the host name of the destination, the device translates *host* into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits, in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f repeatedly to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, like 0x010203…feff01….

-q: Specifies that only statistics are displayed. Absence of this keyword indicates that all information is displayed.

-r: Specifies the recording routing information. If this keyword is not specified, routes are not recorded.

-s *packet-size*: Specifies the length (in bytes) of an ICMP echo request, which is in the range of 20 to 8100 and defaults to 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMP echo reply (ECHO-REPLY). If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out. The value is in the range of 0 to 65535 and defaults to 2000.

-tos *tos*: Specifies the ToS value for an echo request, which is in the range of 0 to 255 and defaults to 0.

-v: Displays the non-ICMP echo reply received. If this keyword is not specified, the system does not display non ICMP echo reply.

host: Specifies the IP address or host name (a string of 1 to 255 characters) for the destination.

Description

Use **ping** to verify whether the destination in an IP network is reachable, and to display the related statistics.

With the **ping** command executed, the source sends an ICMP echo request to the destination:

- If the destination name is unrecognizable, the system outputs "Error: Ping: Unknown host *host-name*."
- If the source receives an ICMP echo reply from the destination within the timeout, the system outputs the related information of the reply.
- If the source does not receive an ICMP echo reply from the destination within the timeout, the system outputs "Request time out."
- To use the name of the destination host to perform the ping operation, you must configure the Domain Name System (DNS) on the device first. Otherwise, the ping operation fails. In addition, you must use the command in the form of **ping ip** *ip* instead of **ping** *ip* if the destination name is a key word, such as **ip**.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

# Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Sysname> ping 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/41/205 ms
```

The output shows the following:

- The destination was reachable.
- All ICMP echo requests sent by the source got responses.
- The minimum time, average time, and maximum time for the packet's roundtrip time are 1 ms, 41 ms, and 205 ms respectively.

# Test whether the device with an IP address of 1.1.2.2 is reachable. Only the check results are displayed.

```
<Sysname> ping -q 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/12/29 ms
```

# Test whether the device with an IP address of 1.1.2.2 is reachable. The route information is displayed.

```
<Sysname> ping -r 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=53 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
```

```
        1.1.1.2
        1.1.1.1

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/11/53 ms
```

The output shows the following:

- The destination was reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 1 Command output

Field	Description
PING 1.1.2.2	Test whether the device with IP address 1.1.2.2 is reachable.
56 data bytes	Number of data bytes in each ICMP echo request.
press CTRL_C to break	During the execution of the command, you can press **Ctrl+C** to abort the ping operation.
Reply from 1.1.2.2 : bytes=56 Sequence=1 ttl=255 time=1 ms	Received the ICMP reply from the device whose IP address is 1.1.2.2. If no reply is received during the timeout period, "Request time out" is displayed. • **bytes**—Indicates the number of data bytes in the ICMP reply. • **Sequence**—Indicates the packet sequence, used to determine whether a segment is lost, disordered or repeated. • **ttl**—Indicates the TTL value in the ICMP reply. • **time**—Indicates the response time.
Record Route:	Routers through which the ICMP echo request passed. They are displayed in inversed order. The router with a smaller distance to the destination is displayed first.
-- 1.1.2.2 ping statistics --	Statistics on data received and sent in the ping operation.
5 packet(s) transmitted	Number of ICMP echo requests sent.
5 packet(s) received	Number of ICMP echo requests received.
0.00% packet loss	Percentage of packets not responded to the total packets sent.
round-trip min/avg/max = 0/4/20 ms	Minimum/average/maximum response time, in ms. The field is not available for failed ping attempts in an IPv4 network. In an IPv6 network, however, the field is available and set to **0/0/0 ms**.

ping ipv6

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos*] * *host* [**-i** *interface-type interface-number*]

View

Any view

Default level

0: Visit level

Parameters

-a *source-ipv6*: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device. If this option is not specified, the source IPv6 address of an ICMP echo request is the primary IPv6 address of the outbound interface of the request.

-c *count*: Specifies the number of times that an ICMPv6 echo request is sent, which is in the range of 1 to 4294967295 and defaults to 5.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, which is in the range of 1 to 65535 and defaults to 200.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-s *packet-size*: Specifies the length (in bytes) of an ICMPv6 echo request, which is in the range of 20 to 8100 and defaults to 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMPv6 echo reply, which is in the range of 0 to 65535 and defaults to 2000.

-tos *tos*: Specifies the ToS value for an IPv6 echo request, which is in the range of 0 to 255 and defaults to 0.

host: Specifies the IPv6 address or host name of the destination, a string of 1 to 46 characters.

-i *interface-type interface-number*: Specifies an outbound interface by its type and number. This parameter can be used only when the destination address is the link local address and the specified outbound interface must have a link local address. For more information about the configuration of a link local address, see *Layer 3—IP Services Configuration Guide*. If this parameter is not provided, the ICMP echo request sending interface is determined by searching the routing table or forwarding table according to the destination IP address.

Description

Use **ping ipv6** to verify whether an IPv6 address is reachable, and display the corresponding statistics.

To use the name of the destination host to perform the ping operation, you must configure DNS on the device first. Otherwise, the ping operation fails. For more information about DNS, see *Layer 3—IP Services Configuration Guide*. You must use the command in the form of **ping ipv6** *ipv6* instead of **ping** *ipv6* if the destination name is an ipv6 name.

To abort the ping ipv6 operation during the execution of the command, press **Ctrl+C**.

Examples

# Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
  PING 2001::2 : 56  data bytes, press CTRL_C to break
    Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64  time = 62 ms
    Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64  time = 26 ms
    Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64  time = 20 ms
    Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64  time = 4 ms
    Reply from 2001::1
    bytes=56 Sequence=5 hop limit=64  time = 16 ms

  --- 2001::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/25/62 ms
```

The "hop limit" field in this prompt information has the same meaning as the "ttl" field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request. For a description of other fields, see Table 1.

tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-tos** *tos* | **-w** *timeout*] * *host*

View

Any view

Default level

0: Visit level

Parameters

-a *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device. If this option is not specified, the source IP address of an ICMP echo request is the primary IP address of the outbound interface of the tracert packet.

-f *first-ttl*: Specifies the first TTL (the allowed number of hops for the first packet). It is in the range of 1 to 255 and defaults to 1, and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, or, the maximum allowed number of hops for a packet. It is in the range of 1 to 255 and defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination, which is in the range of 1 to 65535 and defaults to 33434. You do not need to modify this option.

-q *packet-number*: Specifies the number of probe packets sent each time, which is in the range of 1 to 65535 and defaults to 3.

-tos *tos*: Specifies the ToS value for a tracert packet, which is in the range of 0 to 255 and defaults to 0.

-w *timeout*: Specifies the timeout time of the reply packet of a probe packet, which is in the range of 1 to 65535 milliseconds and defaults to 5000 milliseconds.

host: Specifies the IP address or host name (a string of 1 to 255 characters) for the destination.

Description

Use **tracert** to trace the path that the packets traverse from source to destination.

After having identified network failure with the **ping** command, use the **tracert** command to determine the failed node(s).

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. If a device times out, asterisks (* * *) are displayed.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

# Display the path that the packets traverse from source to destination with an IP address of 1.1.2.2.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
[Sysname] ip unreachables enable
[Sysname] tracert 1.1.2.2
 traceroute to 1.1.2.2(1.1.2.2) 30 hops max,40 bytes packet, press CTRL_C to break
 1  1.1.1.2 673 ms 425 ms 30 ms
 2  1.1.2.2 580 ms 470 ms 80 ms
```

Table 2 Command output

Field	Description
traceroute to 1.1.2.2(1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.
hops max	Maximum number of hops of the probe packets, which can be set through the **-m** keyword.
bytes packet	Number of bytes of a probe packet.
press CTRL_C to break	During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.
1 1.1.1.2 673 ms 425 ms 30 ms	Probe result of the probe packets whose TTL is 1, including the IP address of the first hop and the roundtrip time of three probe packets. The number of packets that can be sent in each probe can be set through the **-q** keyword.

tracert ipv6

Syntax

tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-tos** *tos*| **-w** *timeout*] * *host*

View

Any view

Default level

0: Visit level

Parameters

-f *first-ttl*: Specifies the first TTL, or, the allowed number of hops for the first packet. It is in the range of 1 to 255 and defaults to 1, and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL (the maximum allowed number of hops for a packet). It is in the range of 1 to 255 and defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination, which is in the range of 1 to 65535 and defaults to 33434. It is unnecessary to modify this option.

-q *packet-number*: Specifies the number of probe packets sent each time, which is in the range of 1 to 65535 and defaults to 3.

-w *timeout*: Specifies the timeout time of the reply packet of a probe packet, which is in the range of 1 to 65535 milliseconds and defaults to 5000 milliseconds.

host: Specifies the IPv6 address or host name of the destination, a string of 1 to 46 characters.

-tos *tos*: Specifies the ToS value for an IPv6 tracert packet, which is in the range of 0 to 255 and defaults to 0.

Description

Use **tracert ipv6** to view the path the IPv6 packets traverse from source to destination.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices the packets traverse from source to destination. If a device times out, asterisks (* * *) are displayed.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

# View the path the packets traverse from source to destination with IPv6 address 2001::1.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
[Sysname] ip unreachables enable
[Sysname] tracert ipv6 2001::1
 traceroute to 2001::1  30 hops max,60 bytes packet, press CTRL_C to break
 1  2001::1 3 ms <1 ms 19 ms
```

For a description of the fields in the output, see Table 2.

System debugging commands

debugging

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

### View

User view

Default level

1: Monitor level

Parameters

all: All debugging functions.

module-name: Module name, such as arp or device. To display the current module name, use the **debugging ?** command.

option: The debugging option for a specific module. Different modules have different debugging options in terms of their number and content. To display the currently supported options, use the **debugging** *module-name* **?** command.

Description

Use **debugging** to enable the debugging of a specific module.

Use **undo debugging** to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Output of the debugging information may degrade system efficiency, so you should enable the debugging of the corresponding module for diagnosing network failure, and not to enable debugging of multiple modules at the same time.

Default level describes the default level of the **debugging all** command. Different **debugging** commands may have different default levels.

Configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the terminal. For more information about the **terminal debugging** and **terminal monitor** commands, see "Information center configuration commands."

Related commands: **display debugging**.

Examples

# Enable IP packet debugging.

```
<Sysname> debugging ip packet
```

display debugging

Syntax

display debugging [**interface** *interface-type interface-number*] [*module-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the debugging settings of the specified interface, where the *interface-type interface-number* argument represents the interface type and number.

module-name: Module name.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display debugging** to display enabled debugging functions.

Related commands: **debugging**.

Examples

# Display all enabled debugging functions.

```
<Sysname> display debugging
IP packet debugging is on
```

NTP configuration commands

display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about all NTP sessions. If you do not specify this keyword, the command only displays the brief information about the NTP sessions.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see Fundamentals Configuration Guide.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntp-service sessions** to display information about all NTP sessions.

Examples

# Display the brief information of all NTP sessions.

```
<Sysname> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
********************************************************************************
[12345]127.127.1.0     127.127.1.0        3     1   64   33    0.0    0.0    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table 3 Command output

Field	Description
source	IP address of the clock source

Field	Description
reference	Reference clock ID of the clock source. • If the reference clock is the local clock, the value of this field is related to the value of the **stra** field: ○ When the value of the **stra** field is 0 or 1, this field is "LOCL". ○ When the **stra** field has another value, this field is the IP address of the local clock. • If the reference clock is the clock of another device on the network, the value of this field is the IP address of that device.
stra	Stratum level of the clock source, which determines the clock precision. The value ranges from 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
reach	Reachability count of the clock source. A value of 0 indicates that the clock source in unreachable.
poll	Poll interval in seconds, namely, the maximum interval between successive NTP messages.
now	Length of time from when the last NTP message was received or when the local clock was last updated to the current time The time is in seconds by default. If the time length is greater than 2048 seconds, it is displayed in minutes; if greater than 300 minutes, in hours; if greater than 96 hours, in days.
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the clock source, in milliseconds.
disper	Maximum error of the system clock relative to the reference source.
[12345]	• **1**—Clock source selected by the switch, namely, the current reference source. • **2**—Stratum level of the clock source is less than or equal to 15. • **3**—This clock source has survived the clock selection algorithm. • **4**—This clock source is a candidate clock source. • **5**—This clock source was created by a configuration command.
Total associations	Total number of associations.

# Display the detailed information about all NTP sessions.

```
<Sysname> display ntp-service sessions verbose
 clock source: 127.127.1.0
 clock stratum: 3
 clock status: configured, master, sane, valid
 reference clock ID: 127.127.1.0
 local mode: client, local poll: 6
 peer mode: server, peer poll: 6
 offset: 0.0000 ms,delay: 0.00 ms,  disper: 0.02 ms
 root delay: 0.00 ms, root disper: 10.00 ms
 reach: 1, sync dist: 0.010, sync state: 2
 precision: 2^18, version: 3, peer interface: InLoopBack0
```

```
reftime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71484513)
orgtime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71484513)
rcvtime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.7149E881)
xmttime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71464DC2)
filter delay :  0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filter offset:  0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filter disper:  0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
Total associations : 1
```

Table 4 Command output

Field	Description
clock source	IP address of the clock source.
clock stratum	Stratum level of the clock source, which determines the clock precision. The value ranges from 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
clock status	Status of the clock source corresponding to this session, which can be one of the following: • **configured**—The session was created by a configuration command. • **dynamic**—This session is established dynamically. • **master**—The clock source is the primary reference source of the current system. • **selected**—The clock source has survived the clock selection algorithm. • **candidate**—The clock source is the candidate reference source. • **sane**—The clock source has passed the sane authentication. • **insane**—The clock source has failed the sane authentication. • **valid**—The clock source is valid, which means the clock source meet the following requirements: it has passed the authentication and is being synchronized; its stratum level is valid; and its root delay and root dispersion values are within their ranges. • **invalid**—The clock source is invalid. • **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.
reference clock ID	Reference clock ID of the clock source. • If the reference clock is the local clock, the value of this field is related to the stratum level of the clock source: ○ When the stratum level of the clock source is 0 or 1, this field is "LOCL". ○ When the stratum level of the clock source has another value, this field is the IP address of the local clock. • If the reference clock is the clock of another device on the network, the value of this field is the IP address of that device.

Field	Description
local mode	Operation mode of the local device, which can be one of the following: - **unspec**—The mode is unspecified. - **active**—Active mode. - **passive**—Passive mode. - **client**—Client mode. - **server**—Server mode. - **bdcast**—Broadcast server mode. - **control**—Control query mode. - **private**—Private message mode.
local poll	Poll interval of the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 26, or 64 seconds.
peer mode	Operation mode of the peer device, which can be one of the following: - **unspec**—The mode is unspecified. - **active**—Active mode. - **passive**—Passive mode. - **client**—Client mode. - **server**—Server mode. - **bdcast**—Broadcast server mode. - **control**—Control query mode. - **private**—Private message mode.
peer poll	Poll interval of the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 26, or 64 seconds.
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the clock source, in milliseconds.
disper	Maximum error of the system clock relative to the reference clock.
root delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
root disper	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
reach	Reachability count of the clock source. A value of 0 indicates that the clock source is unreachable.
sync dist	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
sync state	State of the state machine. The displayed value is an integer that ranges from 0 to 5.
precision	Precision of the system clock.

Field	Description
version	NTP version. The displayed value is an integer that ranges from 1 to 4.
peer interface	Source interface. If the source interface is not specified, this field is **wildcard**.
reftime	Reference timestamp in the NTP message.
orgtime	Originate timestamp in the NTP message.
rcvtime	Receive timestamp in the NTP message.
xmttime	Transmit timestamp in the NTP message.
filter delay	Delay information.
filter offset	Offset information.
filter disper	Dispersion information.
Total associations	Total number of associations.

NOTE:

When a device is operating in NTP broadcast/multicast server mode, executing the **display ntp-service sessions** command on the device does not display the NTP session information corresponding to the broadcast/multicast server, but the sessions are counted in the total number of associations.

display ntp-service status

Syntax

display ntp-service status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see Fundamentals Configuration Guide.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntp-service status** to display the NTP service status information.

Examples

# Display the NTP service status information.

```
<Sysname> display ntp-service status
```

```
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

Table 5 Command output

Field	Description
Clock status	Status of the system clock, which can be one of the following: - **Synchronized**—The system clock has been synchronized. - **Unsynchronized**—The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock.
Reference clock ID	When the system clock is synchronized to a remote time server, this field indicates the address of the remote time server. When the system clock is synchronized to a local reference source, this field indicates the address of the local clock source: - When the local clock has a stratum level of 1, the value of this field is "LOCL". - When the stratum of the local clock has another value, the value of this field is the IP address of the local clock.
Nominal frequency	Nominal frequency of the local system hardware clock, in Hz.
Actual frequency	Actual frequency of the local system hardware clock, in Hz.
Clock precision	Precision of the system clock.
Clock offset	Offset of the system clock relative to the reference source, in milliseconds.
Root delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
Root dispersion	Maximum error of the system clock relative to the primary reference source, in milliseconds.
Peer dispersion	Maximum error of the system clock relative to the reference source, in milliseconds.
Reference time	Reference timestamp.

display ntp-service trace

Syntax

display ntp-service trace [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see Fundamentals Configuration Guide.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntp-service trace** to display the brief information about each NTP server from the local device back to the primary reference source.

The **display ntp-service trace** command takes effect only when the local device and all the devices on the NTP server chain can reach one another. Otherwise, this command is unable to display all the NTP servers on the NTP chain due to timeout.

Examples

# Display the brief information about each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid LOCL
```

The output shows an NTP server chain for server 127.0.0.1: Server 127.0.0.1 is synchronized to server 133.1.1.1, and server 133.1.1.1 is synchronized to the local clock source.

Table 6 Command output

Field	Description
server	IP address of the NTP server.
stratum	Stratum level of the corresponding system clock.
offset	Clock offset relative to the upper-level clock, in seconds.
synch distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as "LOCL". Otherwise, it is displayed as the IP address of the primary reference clock.

ntp-service access

Syntax

ntp-service access { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service access { **peer** | **query** | **server** | **synchronization** }

View

System view

Default level

3: Manage level

Parameters

peer: Permits full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

query: Permits control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

server: Permits server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

synchronization: Permits server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

acl-number: Basic ACL number, which ranges from 2000 to 2999.

Description

Use **ntp-service access** to configure the access-control right for the peer devices to access the NTP services of the local device.

Use **undo ntp-service access** to remove the configured NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it matches against the access-control right in this order and uses the first matched right.

The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.

Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.

Examples

# Configure the peer devices on subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
```

```
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service authentication enable** to enable NTP authentication.

Use **undo ntp-service authentication enable** to disable NTP authentication.

By default, NTP authentication is disabled.

Related commands: **ntp-service authentication-keyid** and **ntp-service reliable authentication-keyid**.

Examples

# Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** [**cipher** | **simple**] *value*

undo ntp-service authentication-keyid *keyid*

View

System view

Default level

3: Manage level

Parameters

keyid: Authentication key ID, in the range of 1 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for secrecy.

value: Specifies the MD5 authentication key string. This argument is case sensitive. If **simple** is specified, it is a string of 1 to 32 characters. If **cipher** is specified, it is a string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Description

Use **ntp-service authentication-keyid** to set the NTP authentication key.

Use **undo ntp-service authentication-keyid** to remove the set NTP authentication key.

By default, no NTP authentication key is set.

In a network where there is a high security demand, the NTP authentication feature should be enabled for a system running NTP. This feature enhances the network security by means of the client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.

When the NTP authentication key is configured, configure the key as a trusted key by using the **ntp-service reliable authentication-keyid** command.

Presently the system supports only the MD5 algorithm for key authentication.

A maximum of 1,024 keys can be set for each device.

If an NTP authentication key is specified as a trusted key, the key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

Related commands: **ntp-service reliable authentication-keyid**.

Examples

# Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

View

VLAN interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service broadcast-client** to configure the device to operate in NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use **undo ntp-service broadcast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

# Configure the device to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

View

VLAN interface view

Default level

3: Manage level

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients, where keyid ranges from 1 to 4294967295. This parameter is not meaningful if authentication is not required.

version *number*: Specifies the NTP version, where number ranges from 1 to 4 and defaults to 3.

Description

Use **ntp-service broadcast-server** to configure the device to operate in NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use **undo ntp-service broadcast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

# Configure the device to operate in broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 3
```

ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the Differentiated Services Code Point (DSCP) value for NTP messages, in the range of 0 to 63.

Description

Use the **ntp-service dscp** command to set the DSCP value for NTP messages.

Use the **undo ntp-service dscp** command to restore the default.

By default, the DSCP value for NTP messages is 16.

Examples

# Set the DSCP value to 30 for NTP messages.

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

ntp-service in-interface disable

Syntax

ntp-service in-interface disable

undo ntp-service in-interface disable

View

VLAN interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service in-interface disable** to disable an interface from receiving NTP messages.

Use **undo ntp-service in-interface disable** to restore the default.

By default, all interfaces are enabled to receive NTP messages.

Examples

# Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

View

System view

Default level

3: Manage level

Parameters

number: Maximum number of dynamic NTP sessions that are allowed to be established, which ranges from 0 to 100.

Description

Use **ntp-service max-dynamic-sessions** to set the maximum number of dynamic NTP sessions that are allowed to be established locally.

Use **undo ntp-service max-dynamic-sessions** to restore the maximum number of dynamic NTP sessions to the system default.

By default, the number is 100.

A single device can have a maximum of 128 concurrent associations, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association is removed if the system fails to receive messages from it over a specific long period of time. In client/server mode, for example, when you carry out a command to synchronize the time to a server, the system creates a static association, and the server just responds passively upon the receipt of a message, rather than creating an association (static or dynamic). In symmetric mode, static associations are created at the symmetric-active peer side, and dynamic associations are created at the symmetric-passive peer side. In broadcast or multicast mode, static associations are created at the server side, and dynamic associations are created at the client side.

Examples

# Set the maximum number of dynamic NTP sessions allowed to be established to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

View

VLAN interface view

Default level

3: Manage level

Parameters

ip-address: Multicast IP address, which defaults to 224.0.1.1.

Description

Use **ntp-service multicast-client** to configure the device to operate in NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use **undo ntp-service multicast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

# Configure the device to operate in multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

View

VLAN interface view

Default level

3: Manage level

Parameters

ip-address: Multicast IP address, which defaults to 224.0.1.1.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages, where ttl-number is in the range of 1 to 255 and defaults to 16.

version *number*: Specifies the NTP version, where number is in the range of 1 to 4 and defaults to 3.

Description

Use **ntp-service multicast-server** to configure the device to operate in NTP multicast server mode and use the current interface to send NTP multicast packets.

Use **undo ntp-service multicast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

# Configure the device to operate in multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 3
authentication-keyid 4
```

ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

View

System view

Default level

3: Manage level

Parameters

keyid: Authentication key number, in the range of 1 to 4294967295.

Description

Use **ntp-service reliable authentication-keyid** to specify that the created authentication key is a trusted key. When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use **undo ntp-service reliable authentication-keyid** to remove the configuration.

By default, no authentication key is configured to be trusted.

Examples

# Enable NTP authentication, specify the use of MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
```

# Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax

ntp-service source-interface *interface-type interface-number*

undo ntp-service source-interface

View

System view

Default level

3: Manage level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **ntp-service source-interface** to specify the source interface for NTP messages.

Use **undo ntp-service source-interface** to restore the default.

By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of NTP messages.

If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, use this command to specify the source interface for NTP messages so that the source IP address in NTP messages is the primary IP address of this interface.

Examples

# Specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service source-interface vlan-interface 1
```

ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *ip-address* | *peer-name* }

View

System view

Default level

3: Manage level

Parameters

peer-name: Host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where keyid is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to its peer, the source IP address is the primary IP address of this interface. interface-type interface-number represents the interface type and number.

version *number*: Specifies the NTP version, where number is in the range of 1 to 4 and defaults to 3.

Description

Use **ntp-service unicast-peer** to designate a symmetric-passive peer for the device.

Use **undo ntp-service unicast-peer** to remove the symmetric-passive peer designated for the device.

By default, no symmetric-passive peer is designated for the device.

Examples

# Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, configure the device to run NTP version 3, and specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interface vlan-interface 1
```

ntp-service unicast-server

Syntax

ntp-service unicast-server { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *ip-address* | *server-name* }

View

System view

Default level

3: Manage level

Parameters

server-name: Host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where keyid is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to the NTP server, the source IP address is the primary IP address of this interface. interface-type interface-number represents the interface type and number.

version *number*: Specifies the NTP version, where number is in the range of 1 to 4 and defaults to 3.

Description

Use **ntp-service unicast-server** to designate an NTP server for the device.

Use **undo ntp-service unicast-server** to remove an NTP server designated for the device.

By default, no NTP server is designated for the device.

Examples

# Designate NTP server 10.1.1.1 for the device, and configure the device to run NTP version 3.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```

Information center configuration commands

display channel

Syntax

display channel [*channel-number* | *channel-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Table 7 Information channels for different output destinations

Output destination	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP module	5	snmpagent
Web interface	6	channel6

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display channel** to display channel information.

If no channel is specified, the command displays information about all channels.

Examples

# Display information about channel 0.

```
<Sysname> display channel 0
```

```
channel number:0, channel name:console
MODU_ID   NAME     ENABLE LOG_LEVEL         ENABLE TRAP_LEVEL     ENABLE DEBUG_LEVEL
ffff0000 default  Y      informational     Y      debugging      Y      debugging
```

The output shows that the system is allowed to output log information with a severity from 0 to 4, trap information with a severity from 0 to 7, and debug information with a severity from 0 to 7 to the console. The information source modules are all modules (default).

Table 8 Command output

Field	Description
channel number	Channel number, in the range of 0 to 9.
channel name	Channel name. For more information, see **info-center channel name**.
MODU_ID	ID of the source module.
NAME	Name of the source module. "default" means all modules are allowed to output system information, but the actual permitted modules depends on the switch model.
ENABLE	Indicates whether log output is enabled, Y or N.
LOG_LEVEL	Log information severity. See Table 10 for details.
ENABLE	Indicates whether trap output is enabled, Y or N.
TRAP_LEVEL	Trap information severity See Table 10 for details.
ENABLE	Indicates whether debug output is enabled, Y or N.
DEBUG_LEVEL	Debug information severity. See Table 10 for details.

display info-center

Syntax

display info-center [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display info-center** to display information center configuration information.

Examples

# Display information center configuration information.

```
<Sysname> display info-center
Information Center:enabled
Log host:
    1.1.1.1,
    port number : 514, host facility : local7,
    channel number : 2, channel name : loghost
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 512, dropped messages 0, overwritten messages 740
    channel number : 4, channel name : logbuffer
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
    current messages 216, dropped messages 0, overwritten messages 0
    channel number : 3, channel name : trapbuffer
syslog:
    channel number:6, channel name:channel6
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date
```

Table 9 Command output

Field	Description
Information Center	Information center state, including: • **enabled**—Logs can be output to the information center. • **disabled**—Logs cannot be output to the information center.
Log host: 1.1.1.1, port number : 514, host facility : local2, channel number : 8, channel name : channel8	Configurations on the log host destination (which can be displayed only when the **info-center loghost** command is configured), including IP address of the log host, number of the port that receives the system information on the log host, logging facility used, and the channel number and channel name used.)
Console: channel number : 0, channel name : console	Configurations on the console destination, including the channel number and channel name used.
Monitor: channel number : 1, channel name : monitor	Configurations on the monitor terminal destination, including the channel number and channel name used.

Field	Description
SNMP Agent: channel number : 5, channel name : snmpagent	Configurations on the SNMP module destination, including the channel number and channel name used.
Log buffer: enabled,max buffer size 1024, current buffer size 512, current messages 512, dropped messages 0, overwritten messages 740 channel number : 4, channel name : logbuffer	Configurations on the log buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
Trap buffer: enabled,max buffer size 1024, current buffer size 256, current messages 216, dropped messages 0, overwritten messages 0 channel number : 3, channel name : trapbuffer	Configurations on the trap buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
syslog: channel number:6, channel name:channel6	Configurations on the web interface destination, including the channel number, and channel name used.
Information timestamp setting	Time stamp configurations, specifying the time stamp format for log, trap, debug, and log host information.

display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. Without this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7.

Table 10 Severity description

Severity	Value	Description	Corresponding keyword in commands
Emergency	0	The system is unavailable.	**emergencies**
Alert	1	Action must be taken immediately.	**alerts**
Critical	2	Critical condition.	**critical**

Severity	Value	Description	Corresponding keyword in commands
Error	3	Error condition.	**errors**
Warning	4	Warning condition.	**warnings**
Notice	5	Normal but significant condition.	**notifications**
Informational	6	Informational messages.	**informational**
Debug	7	Debug messages.	**debugging**

size *buffersize*: Specifies the number of latest log messages to be displayed, in the range of 1 to 1,024.

slot *slot-number*: Specifies an IRF member ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display logbuffer** to display the state of the log buffer and the log information in the log buffer. Without **size** *buffersize,* the command displays all log information in the log buffer.

Examples

# Display the state and log information about the log buffer.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 127

%Jun 19 18:03:24:55 2011 Sysname IC/7/SYS_RESTART:
System restarted --
…
```

Table 11 Command output

Field	Description
Logging buffer configuration and contents	Current state of the log buffer, enabled or disabled.
Allowed max buffer size	Maximum number of messages that can be stored in the log buffer.
Actual buffer size	Actual buffer size.
Channel number	Channel number of the log buffer. The default channel number is 4.

Field	Description
Channel name	Channel name of the log buffer. The default channel name is logbuffer.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	Number of current messages.

display logbuffer summary

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7.

slot *slot-number*: Specifies an IRF member ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display logbuffer summary** to display the summary of the log buffer.

Examples

# Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
  SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     1     0     0     0     0     0     0     0     0
     2     0     0     0     0     0     0     0     0
     3     0     0     0     0    16     0     1     0
```

Table 12 Command output

Field	Description
SLOT	ID of an IRF member switch

Field	Description
EMERG	Represents emergency, see Table 10 for details
ALERT	Represents alert, see Table 10 for details
CRIT	Represents critical, see Table 10 for details
ERROR	Represents error, see Table 10 for details
WARN	Represents warning, see Table 10 for details
NOTIF	Represents notice, see Table 10 for details
INFO	Represents informational, see Table 10 for details
DEBUG	Represents debug, see Table 10 for details

display security-logfile buffer

Syntax

display security-logfile buffer [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

User view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display security-logfile buffer** to display the contents of the security log file buffer.

The system buffers security logs into the security log file buffer temporarily. When a saving operation is performed (automatically or manually), the system saves the contents of the security log file buffer into the security log file. After that, the system automatically clears the security log file buffer.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For details of the **authorization-attribute** command, see *Security Command Reference*.

Related commands: **info-center security-logfile frequency** and **security-logfile save**.

Examples

# Display the contents of the security log file buffer.

```
<Sysname> display security-logfile buffer
%@1 Sep 17 11:13:16:609 2011 Sysname SHELL/5/SHELL_LOGIN: Console logged in from aux0.
…
```

display security-logfile summary

Syntax

display security-logfile summary [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Security log management view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display security-logfile summary** to display the summary of the security log file.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, *see Security Command Reference*.

Examples

# Display the summary of the security log file.

```
<Sysname> display security-logfile summary
  Security log file is enabled
  Security log file size quota: 6MB
  Security log file directory: flash:/seclog
  Alarm-threshold: 80%
  Current usage: 30%
  Writing frequency: 1 hour 0 min 0 sec
```

Table 13 Command output

Field	Description
Security log file is	State of the security log file feature, enabled or disabled.
Security log file size quota	Maximum storage space reserved for the security log file.
Security log file directory	Security log file directory.
Alarm-threshold	Alarm threshold of the security log file usage.
Current usage	Current usage of the security log file.
Writing frequency	Security log file writing frequency.

display trapbuffer

Syntax

display trapbuffer [**reverse**] [**size** *buffersize*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

reverse: Displays trap entries chronologically, with the most recent entry at the top. Without this keyword, the command displays trap entries chronologically, with the oldest entry at the top.

size *buffersize*: Specifies the number of latest trap messages to be displayed, in the range of 1 to 1,024.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display trapbuffer** to display the state and the trap information of the trap buffer. Without the **size** *buffersize* argument, the command displays all trap information.

Examples

# Display the state and trap information of the trap buffer. (The actual command output depends on the operations executed on the switch.)

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 9

#Jan  7 08:03:27:421 2011 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983041 is Up, ifAdminStatus is 1,
ifOperStatus is 1
```

Table 14 Command output

Field	Description
Trapping buffer configuration and contents	State of the trap buffer, enabled or disabled.
Allowed max buffer size	Maximum capacity of the trap buffer.

Field	Description
Actual buffer size	Actual capacity of the trap buffer.
Channel number	Channel number of the trap buffer, which defaults to 3.
channel name	Channel name of the trap buffer, which defaults to trapbuffer.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	Number of current messages.

enable log updown

Syntax

enable log updown

undo enable log updown

View

Layer 2 Ethernet interface view, and VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **enable log updown** to allow a port to generate link up/down logs when the port state changes.

Use **undo enable log updown** to disable a port from generating link up/down logs when the port state changes.

By default, all the ports are allowed to generate port link up/down logging information when the port state changes.

Examples

# Disable port GigabitEthernet1/0/1 from generating link up/down logs.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center channel name

Syntax

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel name, a case-insensitive string of 1 to 30 characters. It must be a combination of letters and numbers and start with a letter.

Description

Use **info-center channel name** to name a channel.

Use **undo info-center channel** to restore the default name for a channel.

See Table 7 for information about default channel names and channel numbers.

Examples

# Name channel 0 as **abc**.

```
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center console channel** to specify the console output channel. The system uses this channel to output information to the console.

Use **undo info-center console channel** to restore the default console output channel.

By default, the console output channel is channel 0.

The **info-center console channel** command takes effect only when the information center has been enabled with the **info-center enable** command.

Examples

# Specify the console output channel as channel 0.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

info-center enable

Syntax

info-center enable

undo info-center enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

The switch can output system information only after the information center is enabled.

By default, the information center is enabled.

Examples

# Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
Info: Information center is enabled.
```

info-center format unicom

Syntax

info-center format unicom

undo info-center format

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center format unicom** to set the UNICOM format for system information sent to a log host.

Use **undo info-center format** to restore the default.

By default, the format for the system information sent to a log host is HP.

System information sent to a log host has two formats: HP and UNICOM. For more information, see *Network Management and Monitoring Configuration Guide*.

Examples

# Set the UNICOM format for system information sent to a log host.

```
<Sysname> system-view
[Sysname] info-center format unicom
```

info-center logbuffer

Syntax

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

buffersize: Specifies the maximum number of log messages that can be stored in the log buffer, in the range of 0 to 1024.

Description

Use **info-center logbuffer** to configure information output to the log buffer.

Use **undo info-center logbuffer** to disable information output to the log buffer.

By default, the system outputs information to the log buffer through channel 4 (logbuffer), and the default buffer size is 512.

The **info-center logbuffer** command takes effect only when the information center has been enabled with the **info-center enable** command.

Examples

# Output system information to the log buffer through channel 4, and set the log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

info-center loghost

Syntax

info-center loghost { *host-ipv4-address* | **ipv6** *host-ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*] *

undo info-center loghost { *host-ipv4-address* | **ipv6** *host-ipv6-address* }

View

System view

Default level

2: System level

Parameters

ipv6 *host-ipv6-address*: Specifies the IPv6 address of a log host.

host-ipv4-address: Specifies the IPv4 address of a log host.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default value is 514. It must be the same as the value configured on the log host. Otherwise, the log host cannot receive system information.

dscp *dscp-value:* Specifies the DSCP priority of the packets sent to the log host in the range of 0 to 63. The default value is 0.

channel: Specifies the channel through which system information is output to the log host.

channel-number: Specifies a channel number, in the range of 0 to 9.

channel-name: Specifies a channel name, a default name or a self-defined name. For how to configure a channel name, see the **info-center channel name** command.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filer logs.

Description

Use **info-center loghost** to specify a log host and configure output parameters.

Use **undo info-center loghost** to restore the default.

By default, no log host is specified.

If you configure this command without specifying a channel, the system specifies channel 2 (loghost) by default.

The **info-center loghost** command takes effect only when the information center has been enabled with the **info-center enable** command.

Input a correct log host IP address. The system prompts an invalid address if the loopback address 127.0.0.1 is input.

The switch supports up to four log hosts.

Examples

# Output log information to the log host 1.1.1.1.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

# Output log information to the log host 1::1.

```
<Sysname> system-view
[Sysname] info-center loghost ipv6 1::1
```

info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

View

System view

Default level

2: System level

Parameters

interface-type interface-number: Specifies the egress interface for log information by the interface type and interface number.

Description

Use **info-center loghost source** to specify the source IP address for output log information.

Use **undo info-center loghost source** to restore the default.

By default, the source IP address of output log information is the primary IP address of the matching route's egress interface.

The system uses the primary IP address of the specified egress interface as the source IP address of log information no matter which physical interface is used to output the log information. If you want to display the source IP address in the log information, you can configure it by using this command.

The **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.

The IP address of the specified egress interface must have been configured. Otherwise, although the **info-center loghost source** command can be configured successfully, the log host cannot receive any log information.

Examples

When no source IP address is specified for log information, log in to the FTP server using the username ftp. The following log information is displayed on the log host:

```
<189>Jan 31 05:37:52 2011 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has
logged in successfully.
```

# Specify the IP address of the VLAN interface as the source IP address of log information.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] interface Vlan-interface 100
[Sysname-Vlan-interface100] ip address 2.2.2.2 24
[Sysname-Vlan-interface100] quit
[Sysname] info-center loghost source Vlan-interface 100
```

After the above configuration, log in to the FTP server by using the username ftp. The following log information is displayed on the log host (the **-DevIP=2.2.2.2** field identifies the source IP address):

```
<189>May 31 05:38:14 2011 Sysname %%10FTPD/5/FTPD_LOGIN(l): -DevIP=2.2.2.2; User ftp
(192.168.1.23) has logged in successfully.
```

info-center monitor channel

Syntax

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number, in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center monitor channel** to configure the monitor channel. The system uses this channel to output information to the monitor.

Use **undo info-center monitor channel** to restore the default monitor output channel.

By default, the system outputs information to the monitor through channel 1 (monitor).

The **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

Examples

# Output system information to the monitor through channel 0.

```
<Sysname> system-view
[Sysname] info-center monitor channel 0
```

info-center security-logfile alarm-threshold

Syntax

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

View

System view

Default level

2: System level

Parameters

usage: Specifies an alarm threshold in the range of 1 to 100.

Description

Use **info-center security-logfile alarm-threshold** to set the alarm threshold of the security log file usage.

Use **undo info-center security-logfile alarm-threshold** to restore the default.

By default, the alarm threshold of the security log file usage is 80. That is, when the usage of the security log file reaches 80%, the system informs the administrator.

When the size of the security log file reaches the upper limit, the system deletes the oldest information and then writes the new information into the security log file buffer. This feature can avoid security log loss by setting an alarm threshold. When the threshold is reached, the system outputs log information to inform the administrator. The administrator can log in to the switch as the security log administrator, and back up the security log file.

Related commands: **info-center security-logfile size-quota**.

Examples

# Set the alarm threshold for security log file usage to 90%.

```
<Sysname> system-view
[Sysname] info-center security-logfile alarm-threshold 90
```

info-center security-logfile enable

Syntax

info-center security-logfile enable

undo info-center security-logfile enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center security-logfile enable** to enable the saving of the security logs into the security log file.

Use **undo info-center security-logfile enable** to restore the default.

By default, the saving of security logs into the security log file is disabled.

This feature enables the system to put security logs into the security log file buffer, and saves the logs from the buffer to the security log file at a specific interval.

Examples

# Enable the saving of the security logs into the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
```

info-center security-logfile frequency

Syntax

info-center security-logfile frequency *freq-sec*

undo info-center security-logfile frequency

View

System view

Default level

2: System level

Parameters

freq-sec: Specifies the saving interval in the range of 1 to 86,400 seconds.

Description

Use **info-center security-logfile frequency** to configure the interval for saving security logs to the security log file.

Use **undo info-center security-logfile frequency** to restore the default interval.

The default saving interval is 600 seconds.

Related commands: **info-center security-logfile enable**.

Examples

# Save security logs to the security log file every 3600 seconds.

```
<Sysname> system-view
[Sysname] info-center security-logfile frequency 3600
```

info-center security-logfile size-quota

Syntax

info-center security-logfile size-quota *size*

undo info-center security-logfile size-quota

View

System view

Default level

2: System level

Parameters

size: Specifies the maximum storage space reserved for the security log file, in MB. The value is in the range of 1 to 10.

Description

Use **info-center security-logfile size-quota** to set the maximum storage space reserved for the security log file.

Use **undo info-center security-logfile size-quota** to restore the default.

By default, the storage space reserved for the security log file is 1 MB.

Related commands: **info-center security-logfile alarm-threshold**.

Examples

# Set the maximum storage space reserved for the security log file to 6 MB.

```
<Sysname> system-view
[Sysname] info-center security-logfile size-quota 6
```

info-center security-logfile switch-directory

Syntax

info-center security-logfile switch-directory *dir-name*

View

Any view

Default level

2: System level

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Description

Use **info-center security-logfile switch-directory** to configure the directory where the security log file is saved.

By default, the directory to save the security log file is the **seclog** directory in the root directory of the flash.

The specified directory must have been created.

This command is used for security log file backup or transition and it cannot survive a system restart or a change of roles of IRF member switches.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, see *Security Command Reference*.

Examples

# Set the directory to save the security log file to **flash:/test**.

```
<Sysname> mkdir test
%Created dir flash:/test.
<Sysname> info-center security-logfile switch-directory flash:/test
```

info-center snmp channel

Syntax

info-center snmp channel { *channel-number* | *channel-name* }

undo info-center snmp channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number, in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center snmp channel** to configure the SNMP output channel. The system uses this channel to output information to the SNMP module.

Use **undo info-center snmp channel** to restore the default SNMP output channel.

By default, the system outputs information to the SNMP module through channel 5 (snmpagent).

For more information about SNMP, see "SNMP configuration commands."

Examples

# Output system information to the SNMP module through channel 6.

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

info-center source

Syntax

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

View

System view

Default level

2: System level

Parameters

module-name: Specifies a module. For instance, to output ARP information, specify this argument as ARP. You can use the **info-center source ?** command to view the modules supported by the switch.

default: Specifies all the modules, which can be displayed by using the **info-center source ?** command.

debug: Specifies debug information.

log: Specifies log information.

trap: Specifies trap information.

level *severity*: Specifies a severity level. See Table 10 for more information.

state *state*: Specifies whether to output the specified system information, **on** (enabled) or **off** (disabled).

channel-number: Specifies a channel by its number, in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center source** to configure an information output rule for a module.

Use **undo info-center source** to remove the specified output rule.

The default output rules are listed in Table 15.

This command sets an output rule for a specified module or all modules. For example, you can output IP log information with a severity higher than warning to the log host, and output IP log information with a severity higher than informational to the log buffer.

If you do not set an output rule for a module, the module uses the default output rule or the output rule set by using the **default** keyword.

If you use the **default** keyword to set an output rule for all the modules without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the modules are used. See Table 15 for more information.

If you use the *module-name* argument to set the output rule for a module without specifying the **debug**, **log**, and **trap** keywords, the default settings for the module are as follows: the output of log and trap information is enabled, with *severity* being informational; the output of debugging information is disabled, with *severity* being debug. For example, if you execute the command **info-center source cmd channel** 0, the command is actually equal to the command **info-center source snmp cmd 0 debug level debugging state off log level informational state on trap level informational state on**.

If you repeatedly use the command to set the output rule for a module or for all the modules, the last output rule takes effect

After you set an output rule for a module, you must use the *module-name* argument to modify or remove the rule. A new output rule configured by using the **default** keyword does not take effect for the module.

The trap buffer only receives trap information and discards log and debug information.

The log buffer only receives log and debug information and discards trap information.

The SNMP module only receives trap information and discards log and debug information.

Table 15 Default output rules

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/ disabled	Severity	Enabled/ disabled	Severity	Enabled/ disabled	Severity
Console	default (all modules)	Enabled	Informational	Enabled	Debug	Enabled	Debug
Monitor terminal	default (all modules)	Enabled	Informational	Enabled	Debug	Enabled	Debug
Log host	default (all modules)	Enabled	Informational	Enabled	Debug	Disabled	Debug
Trap buffer	default (all modules)	Disabled	Informational	Enabled	Informational	Disabled	Debug
Log buffer	default (all modules)	Enabled	Informational	Disabled	Debug	Disabled	Debug
SNMP module	default (all modules)	Disabled	Debug	Enabled	Informational	Disabled	Debug
Web interface	All supported modules	Enabled	Debug	Enabled	Debug	Disabled	Debug

Examples

# Output VLAN module's trap information with a severity level of at least emergency to the console channel. All other system information cannot be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel console debug state off log state off trap
state off
[Sysname] info-center source vlan channel console trap level emergencies state on
```

info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

By default, synchronous information output is disabled.

If system information is output before you input information at a command line prompt, the system does not display the command line prompt after the system information output.

If system information is output when you are inputting some interactive information (non Y/N confirmation information), the system displays your input in a new line after the system information output.

Examples

# Enable synchronous information output, and then issue the **display current-configuration** command to view the current configuration of the switch.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%Jan 21 14:33:19:425 2011 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Sysname] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press **Enter** to execute the command.

# Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%Jan 21 14:33:19:425 2011 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

info-center syslog channel

Syntax

info-center syslog channel { *channel-number* | *channel-name* }

undo info-center syslog channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number, in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center syslog channel** to configure the Web output channel. The system uses this channel to output information to the Web interface.

Use **undo info-center syslog channel** to restore the default.

The default Web output channel is channel 6.

Examples

# Output system information to the Web interface through channel 7.

```
<Sysname> system-view
[Sysname] info-center syslog channel 7
```

info-center timestamp

Syntax

info-center timestamp { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }

undo info-center timestamp { **debugging** | **log** | **trap** }

View

System view

Default level

2: System level

Parameters

debugging: Sets the time stamp format for debug information.

log: Sets the time stamp format for log information.

trap: Sets the time stamp format for trap information.

boot: Sets the time stamp format as xxxxxx.yyyyyy, where xxxxxx is the most significant 32 bits (in milliseconds) and yyyyyy is the least significant 32 bits. For example, 0.21990989 equals Jan 25 14:09:26:881 2011. The **boot** time shows the time since system startup.

date: Sets the time stamp format as "Mmm dd hh:mm:ss:sss yyyy". For example, Jan 8 10:12:21:708 2011. The **date** time shows the current system time.

- Mmm: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:sss: Local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Year.

none: Indicates that no time information is provided.

Description

Use **info-center timestamp** to configure the time stamp format for system information sent to all destinations except the log host.

Use **undo info-center timestamp** to restore the default.

By default, the time stamp format for system information sent to a log host is set by the **info-center timestamp loghost** command, and the format for log, trap and debugging information sent to other destinations is **date**.

Related commands: **info-center timestamp loghost**.

Examples

# Configure the time stamp format for log information as **boot**.

```
<Sysname> system-view
[Sysname] info-center timestamp log boot
```

At this time, if you log in to the FTP server by using the username ftp, the log information generated is as follows:

```
%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in
successfully.
```

# Configure the time stamp format for log information as **date**.

```
<Sysname> system-view
[Sysname] info-center timestamp log date
```

At this time, if you log in to the FTP server by using the username ftp, the log information generated is as follows:

```
%Jan 30 05:36:29:579 2011 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged
in successfully.
```

# Configure the time stamp format for log information as **none**.

```
<Sysname> system-view
[Sysname] info-center timestamp log none
```

At this time, if you log in to the FTP server by using the username ftp, the log information generated is as follows:

```
% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully.
```

info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

undo info-center timestamp loghost

View

System view

Default level

2: System level

Parameters

date: Sets the time stamp format as "Mmm dd hh:mm:ss:sss yyyy". For example, Jan 8 10:12:21:708 2011. However, the actual format depends on the log host.

iso: Sets the ISO 8601 time stamp format. For example, 2011-01-21T15:32:55.

no-year-date: Sets the time stamp format as the current system date and time without year.

none: Indicates that no time stamp information is provided.

Description

Use **info-center timestamp loghost** to configure the time stamp format for system information sent to the log host.

Use **undo info-center timestamp loghost** to restore the default.

By default, the time stamp format for system information sent to the log host is **date**.

Related commands: **info-center timestamp**.

Examples

# Configure the time stamp format for system information sent to the log host as **no-year-date**.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

info-center trapbuffer

Syntax

info-center trapbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

View

System view

Default level

2: System level

Parameters

size *buffersize*: Specifies the maximum number of trap messages allowed in the trap buffer, in the range of 0 to 1,024. The default value is 256.

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For how to configure a channel name, see **info-center channel name**.

Description

Use **info-center trapbuffer** to enable information output to the trap buffer and set the corresponding parameters.

Use **undo info-center trapbuffer** to disable information output to the trap buffer.

By default, the system outputs information to the trap buffer through channel 3 (trapbuffer), and the maximum buffer size is 256.

The **info-center trapbuffer** command takes effect only after the information center has been enabled with the **info-center enable** command.

Examples

# Output system information to the trap buffer through the default channel, and set the trap buffer size to 30.

```
<Sysname> system-view
[Sysname] info-center trapbuffer size 30
```

reset logbuffer

Syntax

reset logbuffer

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **reset logbuffer** to clear the log buffer.

Examples

# Clear the log buffer.

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **reset trapbuffer** to clear the trap buffer.

Examples

# Clear the trap buffer.

```
<Sysname> reset trapbuffer
```

security-logfile save

Syntax

security-logfile save

View

Any view

Default level

2: System level

Parameters

None

Description

Use **security-logfile save** to manually save security logs from the security log file buffer into the security log file.

By default, the system automatically saves security logs from the security log file buffer into the security log file at the interval configured by the **info-center security-logfile frequency** command. The directory for the security log file can be configured using the **info-center security-logfile switch-directory** command.

Before backing up the security log file, you can use this command to save the latest security logs in the log buffer into the security log file.

The system clears the security log file buffer after saving security logs into the security log file automatically or manually.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, see *Security Command Reference*.

Examples

# Save the logs in the security log file buffer into the security log file.

```
<Sysname> security-logfile save
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal debugging** to enable the display of debugging information on the current terminal.

Use **undo terminal debugging** to disable the display of debugging information on the current terminal.

By default, the display of debugging information on the current terminal is disabled.

To view debug information, execute the **terminal monitor** and **terminal debugging** commands, enable information center (enabled by default), and finally use a debugging command to enable the related debugging.

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of debugging information on the terminal restores the default.

Examples

# Enable the display of debugging information on the current terminal.

```
<Sysname> terminal debugging
Info: Current terminal debugging is on.
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal logging** to enable the display of log information on the current terminal.

Use **undo terminal logging** to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

To view the log information, execute the **terminal monitor** and **terminal logging** commands, and then enable information center (enabled by default).

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of log information on the terminal restores the default.

Examples

# Disable the display of log information on the current terminal.

```
<Sysname> undo terminal logging
Info: Current terminal logging is off.
```

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal monitor** to enable the monitoring of system information on the current terminal.

Use **undo terminal monitor** to disable the monitoring of system information on the current terminal.

By default, monitoring of the system information on the console is enabled and that on the monitor terminal is disabled.

Configure the **terminal monitor** command before you can display the log, trap, and debugging information.

The **undo terminal monitor** command automatically disables the monitoring of log, trap, and debugging information.

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the monitoring of system information on the terminal restores the default.

Examples

# Enable the monitoring of system information on the current terminal.

```
<Sysname> terminal monitor
Info: Current terminal monitor is on.
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal trapping** to enable the display of trap information on the current terminal.

Use **undo terminal trapping** to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

To view the trap information, execute the **terminal monitor** and **terminal trapping** commands, and then enable information center (enabled by default).

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of trap information on the terminal restores the default.

Examples

# Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
Info: Current terminal trapping is on.
```

SNMP configuration commands

display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

read: Displays information about SNMP read-only communities.

write: Displays information about SNMP read and write communities.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent community** to display SNMPv1 and SNMPv2c community information.

This command displays the SNMPv1 and SNMPv2 communities that you have created by using the **snmp-agent community** command or the **snmp-agent usm-user { v1 | v2c }** command.

Related commands: **snmp-agent community** and **snmp-agent usm-user { v1 | v2c }**.

Examples

# Display information about all SNMPv1 and SNMPv2 communities.

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       Acl:2001
       Storage-type: nonVolatile

   Community name: bb
       Group name: bb
       Storage-type: nonVolatile

   Community name: userv1
       Group name: testv1
       Storage-type: nonVolatile
```

Table 16 Command output

Field	Description
Community name	Displays the community name created by using the **snmp-agent community** command or the username created by using the **snmp-agent usm-user** { **v1** | **v2c** } command.
Group name	SNMP group name. • If the community is created by using the **snmp-agent community** command, the group name is the same as the community name. • If the community is created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, the name of the group to which the user belongs is displayed.
Acl	Number of the ACL that controls the access of the NMSs in the community to the device. Only the NMSs with the IP addresses permitted in the ACL can access the device with the community name.
Storage-type	Storage type: • **volatile**—Settings are lost when the system reboots. • **nonVolatile**—Settings remain after the system reboots. • **permanent**—Settings remain after the system reboots and can be modified but not deleted. • **readOnly**—Settings remain after the system reboots and cannot be modified or deleted. • **other**—Any other storage type.

display snmp-agent group

Syntax

display snmp-agent group [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters. You can specify an SNMPv1, SNMPv2c, or SNMPv3 group.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent group** to display information about an SNMP group, including the group name, security model, MIB view, and storage type. If no group is specified, the command displays information about all SNMP groups.

Examples

# Display information about all SNMP groups.

```
<Sysname> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile
```

Table 17 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: • **authPriv**—authentication with privacy • **authNoPriv**—authentication without privacy • **noAuthNoPriv**—no authentication, no privacy For an SNMPv1 or SNMPv2c group, the security model can be only noAuthNoPriv.
Readview	Read only MIB view accessible to the SNMP group.
Writeview	Writable MIB view associated with the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send traps only for the nodes in the notify MIB view.
Storage-type	Storage type, including volatile, nonVolatile, permanent, readOnly, and other (see Table 16).

display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent local-engineid** to display the local SNMP engine ID.

The local SNMP engine ID uniquely identifies the SNMP engine of the SNMP agent in an SNMP domain.

Every SNMP agent has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

Examples

# Display the local SNMP engine ID.

```
<Sysname> display snmp-agent local-engineid
SNMP local EngineID: 800007DB7F0000013859
```

display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name*: Displays information about the specified MIB view.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent mib-view** to display MIB view information.

If you do not specify any option, the command displays all MIB views.

Examples

# Display all SNMP MIB views of the device.

```
<Sysname> display snmp-agent mib-view
   View name:ViewDefault
```

```
        MIB Subtree:iso
        Subtree mask:
        Storage-type: nonVolatile
        View Type:included
        View status:active

    View name:ViewDefault
        MIB Subtree:snmpUsmMIB
        Subtree mask:
        Storage-type: nonVolatile
        View Type:excluded
        View status:active

    View name:ViewDefault
        MIB Subtree:snmpVacmMIB
        Subtree mask:
        Storage-type: nonVolatile
        View Type:excluded
        View status:active

    View name:ViewDefault
        MIB Subtree:snmpModules.18
        Subtree mask:
        Storage-type: nonVolatile
        View Type:excluded
        View status:active
```

ViewDefault is the default MIB view. The output shows that all MIB objects in the **iso** subtree are accessible except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees.

Table 18 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium where the subtree view is stored.
View Type	Access privilege for the MIB subtree in the MIB view: • **Included**—All objects in the MIB subtree are accessible in the MIB view. • **Excluded**—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view.

display snmp-agent statistics

Syntax

display snmp-agent statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent statistics** to display SNMP message statistics.

Examples

# Display SNMP message statistics.

```
<Sysname> display snmp-agent statistics
  1684 Messages delivered to the SNMP entity
  5 Messages which were for an unsupported version
  0 Messages which used a SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  1679 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
  16544 MIB objects retrieved successfully
  2 MIB objects altered successfully
  7 GetRequest-PDU accepted and processed
  7 GetNextRequest-PDU accepted and processed
  1653 GetBulkRequest-PDU accepted and processed
  1669 GetResponse-PDU accepted and processed
  2 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs dropped silently
  0 Forwarded Confirmed Class PDUs dropped silently
```

Table 19 Command output

Field	Description
Messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
Messages which were for an unsupported version	Number of messages that had an SNMP version not configured on the SNMP agent.
Messages which used a SNMP community name not known	Number of messages that has a community name not configured on the SNMP agent.
Messages which represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages with ASN.1 or BER errors in the process of decoding.
Messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error.
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error.
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error.
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed.
Trap PDUs accepted and processed	Number of traps that have been received and processed.
Alternate Response Class PDUs dropped silently	Number of dropped response packets.
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

contact: Displays the contact information of the current network administrator.

location: Displays the location information of the current device.

version: Displays the version of the current SNMP agent.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent sys-info** to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information is displayed.

Examples

# Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact person for this managed node:
           Hewlett-Packard Development Company, L.P.

   The physical location of this node:

   SNMP version running in the system:
           SNMPv3
```

display snmp-agent trap queue

Syntax

display snmp-agent trap queue [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent trap queue** to display basic information about the trap queue, including trap queue name, queue length and the number of traps in the queue currently.

Related commands: **snmp-agent trap life** and **snmp-agent trap queue-size**.

Examples

# Display the current configuration and usage of the trap queue.

```
<Sysname> display snmp-agent trap queue
   Queue name: SNTP
   Queue size: 100
   Message number: 6
```

Table 20 Command output

Field	Description
Queue name	Trap queue name
Queue size	Trap queue size
Message number	Number of traps in the current trap queue

display snmp-agent trap-list

Syntax

display snmp-agent trap-list [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent trap-list** to display modules that can generate traps and their trap status (**enable** or **disable**).

You can use the **snmp-agent trap enable** command to enable or disable the trap function of a module. For a module that has multiple sub-modules, the trap status is **enable** if the trap function of any of its sub-modules is enabled.

Related commands: **snmp-agent trap enable**.

Examples

# Display the modules that can generate traps and their trap status. (The output of this command depends on the device module.)

```
<Sysname> display snmp-agent trap-list
   arp trap enable
   configuration trap enable
   flash trap enable
   standard trap enable
   system trap enable

   Enable traps: 5; Disable traps: 0
```

display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

engineid *engineid*: Displays SNMPv3 user information for the SNMP engine ID identified by *engineid*. When an SNMPv3 user is created, the system records the current local SNMP entity engine ID. The user becomes invalid when the engine ID changes and becomes valid again when the recorded engine ID is restored.

username *user-name*: Displays information about an SNMPv3 user. The username is case-sensitive.

group *group-name*: Displays SNMPv3 user information for an SNMP group name. The group name is case-sensitive.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display snmp-agent usm-user** to display SNMPv3 user information.

Examples

# Display information about SNMPv3 users.

```
<Sysname> display snmp-agent usm-user
   User name: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active

   User name: userv3code
   Group name: groupv3code
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
```

Table 21 Command output

Field	Description
User name	SNMP username.
Group name	SNMP group name.
Engine ID	Engine ID for an SNMP entity.
Storage-type	Storage type: • volatile • nonvolatile • permanent • readOnly • other For more information, see Table 16.
UserStatus	SNMP user status.

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Layer 2 Ethernet interface view, VLAN interface view

Default level

2: System level

Parameters

None

Description

Use **enable snmp trap updown** to enable link state traps on an interface.

Use **undo enable snmp trap updown** to disable link state traps on an interface.

By default, link state traps are enabled.

For an interface to generate linkUp/linkDown traps when its state changes, you must also enable the linkUp/linkDown trap function globally by using the **enable snmp trap updown** command.

Related commands: **snmp-agent target-host** and **snmp-agent trap enable**.

Examples

# Enable port GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

snmp-agent

Syntax

snmp-agent

undo snmp-agent

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

By default, the SNMP agent is disabled.

The **snmp-agent** command is optional for an SNMP configuration task. The SNMP agent is automatically enabled when you perform any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** and **snmp-agent ifmib long-ifindex enable** commands.

Examples

# Enable the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent
```

snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

Default level

3: Manage level

Parameters

plain-password: Specifies a plaintext authentication or privacy key.

mode: Specifies authentication and privacy algorithms. Select a mode option, depending on the authentication and privacy algorithm you are configuring with the **snmp-agent usm-user v3** command. The three privacy algorithms Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and Data Encryption Standard (DES) are in descending order of security strength. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements. The Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-1) are the two authentication algorithms. MD5 is faster but less secure than SHA-1.

- **3desmd5**: Converts the plaintext privacy key to an encrypted key for 3DES encryption used together with MD5 authentication.
- **3dessha**: Converts the plaintext privacy key to an encrypted key for 3DES encryption used together with SHA-1 authentication.
- **md5**: Converts the plaintext authentication key to an encrypted key for MD5 authentication, or converts the plaintext privacy key to an encrypted key for AES or DES encryption used in conjunction with MD5.
- **sha**: Converts the plaintext authentication key to an encrypted key for SHA-1 authentication, or converts the plaintext privacy key to an encrypted key for AES or DES encryption used in conjunction with SHA-1 authentication.

local-engineid: Uses the local engine ID to calculate the encrypted key. For more information about engine ID-related configuration, see the **snmp-agent local-engineid** command.

specified-engineid: Uses a user-defined engine ID to calculate the cipher text password.

engineid: Specifies an SNMP engine ID as a hexadecimal string. It must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent calculate-password** to convert a plaintext key to an encrypted key for authentication or encryption.

This command helps you calculate encrypted authentication and privacy keys for SNMPv3 users that use encrypted authentication and privacy keys. To create an SNMPv3 user, see the **snmp-agent usm-user v3** command.

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

In SHA mode, the converted encrypted key is a string of 40 hexadecimal characters. If this key is an authentication key, the entire key string is used for authentication. If this key is a privacy key, only the first 32 hexadecimal characters are used for encryption.

The converted key is valid only under the engine ID specified for key conversion.

Related commands: **snmp-agent usm-user v3**.

Examples

# Use the local engine and the MD5 algorithm to convert the plaintext key **authkey** to an encrypted key.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

snmp-agent community

Syntax

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

undo snmp-agent community { **read** | **write** } *community-name*

View

System view

Default level

3: Manage level

Parameters

read: Assigns the specified community the read only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community the read and write access to MIB objects. A read and write community can configure MIB information.

community-name: Specifies the community name, a string of 1 to 32 characters.

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, which is a string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If no MIB view is specified, the specified community can access the MIB objects in the default MIB view **ViewDefault**. To create a MIB view, use the **snmp-agent mib-view** command.

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IP addresses permitted in the ACL can use the specified community name to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the community name to access the SNMP agent.

Description

Use **snmp-agent community** to configure an SNMP community.

Use **undo snmp-agent community** to delete an SNMP community.

This command is for SNMPv1 and SNMPv2c.

A community comprises NMSs and SNMP agents, and is identified by a community name. When devices in a community communicate with each other, they use the community name for authentication. An NMS and an SNMP agent can access each other only when they are configured with the same community name. Typically, **public** is used as the read-only community name, and **private** is used as the read and write community name. To improve security, assign your SNMP communities a name other than **public** and **private**.

To make sure the MIB objects are accessible only to a specific NMS, use a basic ACL to identify the source IP address of the NMS. To set the range of the MIB objects available for the community, use a MIB view.

Related commands: **snmp-agent mib-view**.

Examples

# Create the read-only community **readaccess** so an NMS can use the protocol SNMPv1 or SNMPv2c and community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read readaccess
```

# Create the read and write community **writeaccess** so only the host at 1.1.1.1 can use the protocol SNMPv2c and community name **writeaccess** to read and set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write writeaccess acl 2001
```

# Create the read and write community **wr-sys-acc** so an NMS can use the protocol SNMPv1 or SNMPv2c, community name **wr-sys-acc** to read and set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write wr-sys-acc mib-view test
```

snmp-agent group

Syntax

SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

undo snmp-agent group { **v1** | **v2c** } *group-name*

SNMPv3:

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

System view

Default level

3: Manage level

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies the group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMPv3 group to be authentication only (without privacy).

privacy: Specifies the security model of the SNMPv3 group to be authentication and privacy.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view, which is a string of 1 to 32 characters. The users in the specified group have read only access to the objects included in the MIB view. The default read view is **ViewDefault**.

write-view *view-name:* Specifies a read and write MIB view. The *view-name* argument represents a MIB view, which is a string of 1 to 32 characters. The users in the specified group have read and write access to the objects included in the MIB view. By default, no write view is configured, which means the NMS cannot perform the write operations to all MIB objects on the device.

notify-view *view-name*: Specifies a trap MIB view. The *view-name* argument represents a MIB view, which is a string of 1 to 32 characters. The system sends traps to the users in the specified group for the objects included in the MIB view. By default, no notify view is configured, which means the agent does not send traps to the NMS.

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. In the specified SNMP group, only the NMSs with the IP addresses permitted in the ACL can access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. In the specified SNMP group, only the NMSs with the IPv6 addresses permitted in the ACL can access the SNMP agent.

Description

Use **snmp-agent group** to create an SNMP group and specify its access right.

Use **undo snmp-agent group** to delete an SNMP group.

By default, no SNMP group exists. SNMPv3 groups use the no authentication, no privacy security model if neither **authentication** nor **privacy** is specified.

All the users in an SNMP group share the security model and access rights of the group.

Related commands: **snmp-agent mib-view** and **snmp-agent usm-user**.

Examples

# Create the SNMPv3 group **group1** and assign the no authentication, no privacy security model to the group.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

View

System view

Default level

3: Manage level

Parameters

engineid: Specifies an SNMP engine ID as a hexadecimal string. It must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent local-engineid** to configure the SNMP engine ID of the local SNMP agent.

Use **undo snmp-agent local-engineid** to restore the default local SNMP engine ID.

By default, the local engine ID is the combination of the company ID and the device ID. Device ID varies by product and might be an IP address, a MAC address, or a user-defined hexadecimal string.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP managed network. Make sure that the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

Related commands: **snmp-agent usm-user**.

Examples

# Configure the local engine ID as **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

snmp-agent log

Syntax

snmp-agent log { **all** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **get-operation** | **set-operation** }

View

System view

Default level

3: Manage level

Parameters

all: Enables logging SNMP Get and Set operations.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Description

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to restore the default.

By default, SNMP logging is disabled.

Use SNMP logging to record the SNMP operations performed on the SNMP agent for auditing NMS behaviors. The SNMP agent sends log data to the information center. You can configure the information center to output the data to a specific destination as needed.

Examples

# Enable logging SNMP GET operations.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

# Enable logging SNMP SET operations.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

snmp-agent ifmib long-ifindex enable

Syntax

snmp-agent ifmib long-ifindex enable

undo snmp-agent ifmib long-ifindex enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **snmp-agent ifmib long-ifindex enable** to switch the format of an NM-specific ifindex from 16-bit to 32-bit.

Use **undo snmp-agent ifmib long-ifindex enable** to restore the default.

By default, an NM-specific ifindex is in 16-bit format.

Some configurations use parameters relating to NM-specific ifindex; therefore, the switch of NM-specific ifindex causes temporary ineffectiveness of these configurations (if the format of the ifindex is switched back, the configurations will become effective again). In this case, you need to perform the configurations again with the new NM-specific ifindexes, and then the related configurations become effective. For example, in the configuration of RMON alarm group and private alarm group, the alarm variables are presented in the format of **OID/variable-name.NM-specific-ifindex**; the switching of NM-specific ifindex format makes the RMON alarm variables ineffective. To monitor the affected nodes again, you need to re-configure the alarm groups with the new format of NM-specific ifindexes.

Examples

# Switch the format of an NM-specific ifindex from 16-bit to 32-bit.

```
<Sysname> system-view
[Sysname] snmp-agent ifmib long-ifindex enable
```

snmp-agent mib-view

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

View

System view

Default level

3: Manage level

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to the nodes in the specified MIB subtree.

view-name: Specifies the view name, a string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example **1.4.5.3.1)** or object name (for example, **system**). An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask *mask-value*: Sets a MIB subtree mask, which is a hexadecimal string. Its length must be an even number in the range of 2 to 32. For example, you can specify **0a**, **aa**, but not **0aa**. If no subtree mask is specified, the MIB subtree mask is an all-F hexadecimal string. The MIB subtree and the subtree mask together identify a set of objects to be included or excluded from the view.

Description

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

By default, the system creates the **ViewDefault** view when the SNMP agent is enabled. In the default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the last configuration takes effect.

The system can store entries for up to 20 unique MIB view records. In addition to the four default MIB view records, you can create up to 16 unique MIB view records. After you delete the default view with the **undo snmp-agent mib-view** command, you can create up to 20 unique MIB view records.

Be cautious with deleting the default MIB view. The operation blocks access to any MIB object on the device from NMSs that use the default view.

Related commands: **snmp-agent community** and **snmp-agent group**.

Examples

# Include the **mib-2** (OID 1.3.6.1) subtree in the **mibtest** view and exclude the **ip** subtree from this view.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1
[Sysname] snmp-agent mib-view excluded mibtest ip
[Sysname] snmp-agent community read public mib-view mibtest
```

An SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree, but not any object (for example, the **ipForwarding** or **ipDefaultTTL** node) in the **ip** subtree.

snmp-agent packet max-size

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

View

System view

Default level

3: Manage level

Parameters

byte-count: Specifies the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940, and the default is 1500.

Description

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default packet size.

By default, the maximum size of SNMP packets is 1500 bytes.

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

# Set the maximum SNMP packet size to 1024 bytes.

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1024
```

snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

View

System view

Default level

3: Manage level

Parameters

dscp-value: Specifies the DSCP value for SNMP responses, which ranges from 0 to 63.

Description

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

The default DSCP value for SNMP responses is 0.

Examples

# Set the DSCP value to 45 for SNMP responses.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 45
```

snmp-agent sys-info

Syntax

snmp-agent sys-info { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

undo snmp-agent sys-info { **contact** | **location** | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

View

System view

Default level

3: Manage level

Parameters

contact *sys-contact*: Specifies the system contact, a string of 1 to 200 characters.

location *sys-location*: Specifies the system location, a string of 1 to 200 characters. This information is stored in a management variable in the **system** group defined in RFC1213-MIB.

version: Specifies SNMP versions.

- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3.
- **v1**: Specifies SNMPv1.
- **v2c**: Specifies SNMPv2c.
- **v3**: Specifies SNMPv3.

Description

Use **snmp-agent sys-info** to configure system information for the SNMP agent, including the contact, location, and SNMP versions.

Use **undo snmp-agent sys-info contact** and **undo snmp-agent sys-info location** to restore the default.

Use **undo snmp-agent sys-info version** to disable an SNMP version.

By default, the contact information is **Hewlett-Packard Development Company, L.P**, the location information is null, and the protocol version is **SNMPv3.**.

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

Related commands: **display snmp-agent sys-info**.

Examples

# Configure the system contact as **Dial System Operator at beeper # 27345**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax

snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

View

System view

Default level

3: Manage level

Parameters

trap: Specifies a target host for receiving the traps sent by the SNMP agent.

address: Specifies the IP address of the trap target host.

udp-domain: Specifies UDP as the transport protocol.

ip-address: Specifies the IPv4 address of the target host.

ipv6 *ipv6-address*: Specifies the IPv6 address of the target host.

udp-port *port-number*: Specifies the UDP port for receiving SNMP traps. The default UDP port is 162.

dscp *dscp-value*: Sets the DSCP value for SNMP traps. The value range is 0 to 63 and the default DSCP is 0.

params securityname *security-string*: Specifies the authentication related parameter. The *security-string* argument specifies an SNMPv1 or SNMPv2c community name or an SNMPv3 username, a string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and privacy key when you create the SNMPv3 user.

Description

Use **snmp-agent target-host** to configure a target host for receiving traps sent by the SNMP agent.

Use **undo snmp-agent target-host** to remove settings for an SNMP trap target host.

You can specify up to 20 trap target hosts.

Make sure that the SNMP agent uses the same UDP port number as the target host for traps. If **udp-port** *port-number* is not specified, UDP port 162 is used by default. Port 162 is the SNMP-specified port used for receiving traps, and is used by most NMSs, including iMC and MIB Browser.

Make sure that the SNMP agent uses the same SNMP version as the trap target host so the host can receive traps. If none of the keywords **v1, v2** and **v3** is specified, SNMPv1 is used.

If neither **authentication** nor **privacy** is specified, the authentication mode is no authentication, no privacy.

Related commands: **enable snmp trap updown**, **snmp-agent trap enable**, **snmp-agent trap life**, and **snmp-agent trap source**.

Examples

# Configure the SNMP agent to send SNMPv1 traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [**arp rate-limit** | **configuration** | **default-route** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

undo snmp-agent trap enable [**arp rate-limit** |**configuration** | **default-route** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

View

System view

Default level

3: Manage level

Parameters

arp rate-limit: Enables ARP rate limit traps, which are sent when the ARP packet rate exceeds the rate limit.

configuration: Enables configuration traps.

flash: Enables Flash-related SNMP traps.

default-route: Enables default route traps, which are sent when default routes are deleted.

standard: Enables the sending of standard traps.

- **authentication**: Enables sending authentication failure traps in the event of authentication failure.
- **coldstart**: Sends coldstart traps when the device restarts.
- **linkdown**: Globally enables sending LinkDown traps when the link of a port goes down.
- **linkup**: Globally enables sending LinkUp traps when the link of a port goes up.
- **warmstart**: Sends warmstart traps when the SNMP agent restarts.

system: Enables H3C-SYS-MAN-MIB (an H3C proprietary MIB) traps.

Description

Use **snmp-agent trap enable** to enable traps globally.

Use **undo snmp-agent trap enable** to disable traps globally.

By default, traps are enabled for all modules.

After you globally enable a trap function for a module, whether the module generates traps also depends on the configuration of the module. For more information, see the sections for each module.

To generate Linkup or Linkdown traps when the link state of an interface changes, you must enable the linkUp or linkDown trap function globally by using the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command and on the interface by using the **enable snmp trap updown** command.

Related commands: **snmp-agent target-host** and **enable snmp trap updown**.

Examples

# Enable the SNMP agent to send SNMP authentication failure traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Sysname] snmp-agent trap enable standard authentication
```

snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown traps.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

By default, the SNMP agent sends standard linkUp/linkDown traps.

The extended linkUp and linkDown traps adds interface description and interface type to the standard linkUp and linkDown traps for fast failure point identification. When you configure the **snmp-agent trap if-mib link extended** command, make sure that the NMS supports the extended linkUp and linkDown traps.

- A standard linkUp trap is in the following format:

```
#Jan 24 11:48:04:896 2011 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1,
ifOperStatus is 1
```

- An extended linkUp trap is in the following format:

```
#Jan 24 11:43:09:896 2011 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1,
ifOperStatus is 1, ifDescr is Ethernet1/1, ifType is 6
```

- A standard linkDown trap is in the following format:

```
#Jan 24 11:47:35:224 2011 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2
```

- An extended linkDown trap is in the following format:

```
#Jan 24 11:42:54:314 2011 AR29.46 IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

The format of an extended linkup/ linkDown trap is the standard format followed with the ifDescr and ifType information, facilitating problem location.

When this command is configured, the device sends extended linkUp/linkDown traps. If the extended messages are not supported on NMS, the device may not be able to resolve the messages.

Examples

# Extend standard linkUp/linkDown traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

View

System view

Default level

3: Manage level

Parameters

seconds: Specifies the timeout time, in the range of 1 to 2592000 seconds.

Description

Use **snmp-agent trap life** to configure the holding time of the traps in the queue. Traps are discarded when the holding time expires.

Use **undo snmp-agent trap life** to restore the default holding time of traps in the queue.

By default, the holding time of SNMP traps in the queue is 120 seconds.

The SNMP module sends traps in queues. As soon as the traps are saved in the trap queue, a timer is started. If traps are not sent out until the timer times out (in other words, the holding time configured by using this command expires), the system removes the traps from the trap sending queue.

Related commands: **snmp-agent trap enable** and **snmp-agent target-host**.

Examples

# Configure the holding time of traps in the queue as 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

View

System view

Default level

3: Manage level

Parameters

size: Specifies the number of traps that can be stored in the trap sending queue, in the range of 1 to 1000.

Description

Use **snmp-agent trap queue-size** to set the size of the trap sending queue.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

By default, up to 100 traps can be stored in the trap sending queue.

Traps are saved into the trap sending queue when generated. The size of the queue determines the maximum number of traps that can be stored in the queue. When the size of the trap sending queue reaches the configured value, the newly generated traps are saved into the queue, and the earliest ones are discarded.

Related commands: **snmp-agent target-host**, **snmp-agent trap enable**, and **snmp-agent trap life**.

Examples

# Set the maximum number of traps that can be stored in the trap sending queue to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

View

System view

Default level

3: Manage level

Parameters

interface-type interface-number: Specifies the interface type and interface number.

Description

Use **snmp-agent trap source** to specify the source IP address contained in the traps.

Use **undo snmp-agent trap source** to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the traps.

Upon the execution of this command, the system uses the primary IP address of the specified interface as the source IP address of the traps, and the NMS uses this IP address to uniquely identify the agent. Even if the agent sends out traps through different interfaces, the NMS uses this IP address to filter all traps sent from the agent.

Before you can configure the IP address of a particular interface as the source IP address of the trap, make sure that the interface already exists and that it has a legal IP address. If the configured interface does not exist, the configuration fails. If the specified IP address is illegal, the configuration becomes invalid. When a legal IP address is configured for the interface, the configuration automatically becomes valid.

Related commands: **snmp-agent target-host** and **snmp-agent trap enable**.

Examples

# Configure the IP address for the port Vlan-interface1 as the source address for traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source Vlan-interface1
```

snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

View

System view

Default level

3: Manage level

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2.

user-name: Specifies the username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies the group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. If the group has not been created, the user takes effect after you create the group.

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username (community name) to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username (community name) to access the SNMP agent.

Description

Use **snmp-agent usm-user** { **v1** | **v2c** } to add a user to an SNMPv1 or SNMPv2c group.

Use **undo snmp-agent usm-user** { **v1** | **v2c** } to delete a user from an SNMPv1 or SNMPv2c group.

When you create an SNMPv1 or SNMPv2c user, the system automatically creates a read-only community that has the same name as the SNMPv1 or SNMPv2c username. To change the access right of this community to write access, use the **snmp-agent community** command or the **snmp-agent group** { **v1** | **v2c** } command. To display the SNMPv1 and SNMPv2c communities created in this way, use the **display snmp-agent community** command.

The **snmp-agent usm-user** { **v1** | **v2c** } command enables managing SNMPv1 and SNMPv2c users in the same way as managing SNMPv3 users. It does not affect the way of configuring SNMPv1 and SNMPv2c communities on the NMS.

Related commands: **snmp-agent community** and **snmp-agent group**.

Examples

# Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

# Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the SNMP agent.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [[**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **engineid** *engineid-string* }

View

System view

Default level

3: Manage level

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies the group name, a case-sensitive string of 1 to 32 characters.

cipher: Sets ciphertext authentication and privacy keys, If this keyword is not specified, *auth-password* and *priv-password* must be plaintext keys. To obtain the hexadecimal ciphertext for a key, use the **snmp-agent calculate-password** command.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA. For more information about these algorithms, see *Security Configuration Guide*.

- **md5**: Specifies the MD5 authentication algorithm.
- **sha**: Specifies the SHA-1 authentication protocol algorithm.

auth-password: Specifies the authentication key string. This argument is case sensitive. If **cipher** is not specified, it must be a plaintext string of 1 to 64 characters. If **cipher** is specified, the ciphertext key length requirements differ by authentication algorithm and key string format, as shown in Table 22.

Table 22 Encrypted authentication key length requirements

Authentication algorithm	Hexadecimal string	Non-hexadecimal string
MD5	32 characters	53 characters
SHA	40 characters	57 characters

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des**: Specifies the 3DES algorithm.
- **des56**: Specifies the DES algorithm.
- **aes128**: Specifies the AES algorithm.

priv-password: Specifies the privacy key string. This argument is case sensitive. If **cipher** is not specified, it must be a plaintext string of 1 to 64 characters. If **cipher** is specified, the ciphertext key length requirements differ by authentication algorithm and key string format, as shown in Table 23.

Table 23 Encrypted privacy key length requirements

Authentication algorithm	Encryption algorithm	Hexadecimal string	Non-hexadecimal string
MD5	3DES	64 characters	73 characters
MD5	AES128 or DES-56	32 characters	53 characters
SHA	3DES	80 characters	73 characters
SHA	AES128 or DES-56	40 characters	53 characters

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid *engineid-string*: Specifies the SNMP engine ID as a hexadecimal string. The *engineid-string* argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent usm-user v3** to create an SNMPv3 user in an SNMP group.

Use **undo snmp-agent usm-user v3** to delete an SNMPv3 user from an SNMP group.

You must create an SNMPv3 user for the agent and the NMS to use SNMPv3.

You must create an SNMP group before you assign an SNMP user to the group. Otherwise, the user cannot take effect after it is created. An SNMP group can contain multiple users. It defines SNMP objects accessible to the group of users in the MIB view and specifies whether to enable authentication and privacy functions. The authentication and encryption algorithms are defined when a user is created.

You can use the **snmp-agent calculate-password** command to obtain a hexadecimal ciphertext string for the *pri-password* argument in the **snmp-agent usm-user v3 cipher** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command, make sure that the same privacy protocol is specified for the two commands and the local engine ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity engine ID specified in the **snmp-agent calculate-password** command.

When you execute this command repeatedly to configure the same user (the usernames are the same, no limitation to other keywords and arguments), the last configuration takes effect.

For secrecy, both plaintext and ciphertext keys are saved in cipher text. Remember the username and the plaintext password when you create a user. A plaintext password is required when the NMS accesses the SNMP agent.

Related commands: **snmp-agent calculate-password**, **snmp-agent group**, and **snmp-agent usm-user** { **v1** | **v2c** }.

Examples

# Add the user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication without privacy**, the authentication algorithm as **MD5**, and the plain-text key as **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
```

- Set the SNMP version on the NMS to SNMPv3.
- Fill in the username **testUser**.
- Set the authentication algorithm to **MD5**.
- Set the authentication encrypted key to **authkey**.
- Establish a connection, and the NMS can access the MIB objects in the default view (ViewDefault) on the device.

# Add the user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication and privacy**, the authentication algorithm as MD5, the privacy algorithm as DES56, the plain-text authentication key as **authkey**, and the plain-text privacy key as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
privacy-mode des56 prikey
```

- Set the SNMP version on the NMS to SNMPv3.
- Fill in the username **testUser**.
- Set the authentication algorithm to **MD5**.
- Set the authentication key to **authkey**.
- Set the privacy algorithm to **DES**.
- Set the privacy key to **prikey**.
- Establish a connection, and the NMS can access the MIB objects in the default view (ViewDefault) on the device.

# Add a user **testUser** to the SNMPv3 group **testGroup** with the **cipher** keyword specified. Configure the security model as **authentication and privacy**, the authentication algorithm as MD5, the privacy algorithm as DES56, the plain-text authentication key as **authkey**, and the plain-text privacy key as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
[Sysname] snmp-agent calculate-password prikey mode md5 local-engineid
The secret key is: 800D7F26E786C4BECE61BF01E0A22705
[Sysname] snmp-agent usm-user v3 testUser testGroup cipher authentication-mode md5
09659EC5A9AE91BA189E5845E1DDE0CC privacy-mode des56 800D7F26E786C4BECE61BF01E0A22705
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the username **testUser**,
- Set the authentication algorithm to **MD5**
- Set the authentication key to **authkey**
- Set the privacy algorithm to **DES**
- Set the privacy key to **prikey**
- Establish a connection, and the NMS can access the MIB objects in the default view(ViewDefault) on the device

RMON configuration commands

display rmon alarm

Syntax

display rmon alarm [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an RMON alarm entry, which ranges from 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon alarm** to display the configuration of the specified RMON alarm entry or all RMON alarm entries.

Related commands: **rmon alarm**.

Examples

# Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Samples type          : absolute
  Variable formula      : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval     : 10(sec)
  Rising threshold      : 50(linked with event 1)
  Falling threshold     : 5(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 0
```

Table 24 Command output

Field	Description
AlarmEntry *entry-number* owned by *owner* is *status*	Status of the alarm entry *entry-number* created by the *owner* is *status*: • *entry-number*—Alarm entry, corresponding to the management information base (MIB) node alarmIndex. • *owner*—Owner of the entry, corresponding to the MIB node alarmOwner. • *status*—Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry, while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node alarmStatus.
Samples type	Sampling type (the value can be absolute or delta), corresponding to the MIB node alarmSampleType.
Variable formula	Alarm variable, namely, the monitored MIB node, corresponding to the MIB node alarmVariable.
Sampling interval	Sampling interval, in seconds, corresponding to the MIB node alarmInterval.
Rising threshold	Alarm rising threshold (When the sampling value is greater than or equal to this threshold, a rising alarm is triggered.), corresponding to the MIB node alarmRisingThreshold.
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.), corresponding to the MIB node alarmFallingThreshold.
When startup enables	How an alarm can be triggered, corresponding to the MIB node alarmStartupAlarm.
Latest value	Last sampled value, corresponding to the MIB node alarmValue.

display rmon event

Syntax

display rmon event [*entry-number*] [**\|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an RMON event entry, which ranges from 1 to 65535. If no entry is specified, the configuration of all event entries is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon event** to display the configuration of the specified RMON event entry or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

Related commands: **rmon event**.

Examples

# Display the configuration of the RMON event table.

```
<Sysname> display rmon event
EventEntry 1 owned by user1 is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 25 Command output

Field	Description
EventEntry	Event entry, corresponding to the MIB node eventIndex.
owned by	Event entry owner, corresponding to the MIB node eventOwner.
VALID	Entry status: • **VALID**—The entry is valid. • **UNDERCREATION**—The entry is invalid. The **display rmon** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings. The status value is stored in the MIB node eventStatus.
Description	Event description, corresponding to the MIB node eventDescription.
cause log-trap when triggered	Actions that the system will take when the event is triggered: • **none**—The system will take no action. • **log**—The system will log the event. • **snmp-trap**—The system will send a trap to the NMS. • **log-and-trap**—The system will log the event and send a trap to the NMS. This field corresponds to the MIB node eventType.
last triggered at	Time when the last event was triggered, corresponding to the MIB node eventLastTimeSent.

display rmon eventlog

Syntax

display rmon eventlog [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an event entry, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon eventlog** to display log information for the specified or all event entries.

If *entry-number* is not specified, the log information for all event entries is displayed.

If you use the **rmon event** command to configure the system to log an event when the event is triggered, the event is recorded in the RMON log. You can use this command to display the details of the log table, which includes event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

Examples

# Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
LogEntry 1 owned by null is VALID.
  Generates eventLog 1.1 at 0day(s) 00h:00m:33s.
  Description: The alarm formula defined in prialarmEntry 1,
     uprise 80 with alarm value 85. Alarm sample type is absolute.
  Generates eventLog 1.2 at 0day(s) 00h:42m:03s.
  Description: The alarm formula defined in prialarmEntry 2,
     less than(or =) 5 with alarm value 0. Alarm sample type is delta.
```

Table 26 Command output

Field	Description
LogEntry	Event entry, corresponding to the MIB node logIndex.
owned by	Event entry owner, corresponding to the MIB node eventOwner.
VALID	Entry status: • **VALID**—The entry is valid. • **UNDERCREATION**—The entry is invalid. The **display rmon** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings. The status value is stored in the MIB node eventStatus.
Generates eventLog at	Time when the log was created (time passed since the device was booted), corresponding to the MIB node logTime.
Description	Log description, corresponding to the MIB node logDescription.

This example shows that event 1 generated two logs.

display rmon history

Syntax

display rmon history [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon history** to display RMON history control entry and history sampling information.

After you have created the history control entry on an interface, the system calculates the information of the interface periodically and saves the information to the etherHistoryEntry table. You can use this command to display the entries in this table.

To configure the number of history sampling records that can be displayed and the history sampling interval, use the **rmon history** command.

Related commands: **rmon history**.

Examples

# Display RMON history control entry and history sampling information for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 1 owned by null is VALID
  Samples interface     : GigabitEthernet1/0/1<ifIndex.1>
  Sampling interval     : 10(sec) with 5 buckets max
  Sampled values of record 1 :
    dropevents        : 0          , octets               : 3166
    packets           : 43         , broadcast packets    : 3
    multicast packets : 6          , CRC alignment errors : 0
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
  Sampled values of record 2 :
    dropevents         : 0          , octets               : 834
    packets            : 8          , broadcast packets    : 1
    multicast packets  : 6          , CRC alignment errors : 0
    undersize packets  : 0          , oversize packets     : 0
    fragments          : 0          , jabbers              : 0
    collisions         : 0          , utilization          : 0
  Sampled values of record 3 :
    dropevents         : 0          , octets               : 1001
    packets            : 9          , broadcast packets    : 1
    multicast packets  : 7          , CRC alignment errors : 0
    undersize packets  : 0          , oversize packets     : 0
    fragments          : 0          , jabbers              : 0
    collisions         : 0          , utilization          : 0
  Sampled values of record 4 :
    dropevents         : 0          , octets               : 766
    packets            : 7          , broadcast packets    : 0
    multicast packets  : 6          , CRC alignment errors : 0
    undersize packets  : 0          , oversize packets     : 0
    fragments          : 0          , jabbers              : 0
    collisions         : 0          , utilization          : 0
```

Table 27 Command output

Field	Description
HistoryControlEntry	History control entry, which corresponds to MIB node etherHistoryIndex.
owned by	Entry owner, which corresponds to MIB node historyControlOwner.
VALID	Entry status: **VALID**—The entry is valid. **UNDERCREATION**—The entry is invalid. The **display rmon** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings. The status value is stored in the MIB node historyControlStatus.
Samples Interface	Sampled interface.
Sampling interval	Sampling period, in seconds, which corresponds to MIB node historyControlInterval. The system periodically samples the information of an interface.
buckets max	Maximum number of history table entries that can be saved, corresponding to the MIB node historyControlBucketsGranted. If the specified value of the **buckets** argument exceeds the history table size supported by the device, the supported history table size is displayed. If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one.
Sampled values of record *number*	The (*number*)th statistics recorded in the system cache. Statistics records are numbered according to the order of time they are saved into the cache.
dropevents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.

Field	Description
octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
packets	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
broadcastpackets	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
multicastpackets	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
undersize packets	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
oversize packets	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
jabbers	Number of jabbers received during the sampling period, corresponding to the MIB node etherHistoryJabbers.
collisions	Number of colliding packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

display rmon prialarm

Syntax

display rmon prialarm [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the private alarm entry index, which ranges from 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon prialarm** to display the configuration of the specified private alarm entry or all private alarm entries.

Related commands: **rmon prialarm**.

Examples

# Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Samples type          : absolute
  Variable formula      : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description           : ifUtilization. GigabitEthernet1/0/1
  Sampling interval     : 10(sec)
  Rising threshold      : 80(linked with event 1)
  Falling threshold     : 5(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever
  Latest value          : 85
```

Table 28 Command output

Field	Description
PrialarmEntry	Private alarm table entry.
owned by	Owner of the entry, user1 in this example.
VALID	Entry status: • **VALID**—The entry is valid. • **UNDERCREATION**—The entry is invalid. The **display rmon** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.
Samples type	Sampling type, whose value can be absolute or delta.
Description	Description of the private alarm entry.
Sampling interval	Sampling interval, in seconds. The system performs absolute sample or delta sample to sampling variables according to the sampling interval.
Rising threshold	Alarm rising threshold. An event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm.
When startup enables	How can an alarm be triggered.
This entry will exist	Lifetime of the entry, which can be forever or span the specified period.
Latest value	Count result of the last sample.

display rmon statistics

Syntax

display rmon statistics [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rmon statistics** to display RMON statistics.

This command displays the interface statistics during the period from the time the statistics entry is created to the time the command is executed. The statistics are cleared when the device reboots.

Related commands: **rmon statistics**.

Examples

# Display RMON statistics for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by null is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 43393306  , etherStatsPkts          : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 29 Command output

Field	Description
EtherStatsEntry	Entry of the statistics table, corresponding to MIB node etherStatsIndex.

Field	Description
VALID	Entry status: **VALID**—The entry is valid. **UNDERCREATION**—The entry is invalid. The **display rmon** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings. The status value is stored in the MIB node etherStatsStatus.
Interface	Interface on which statistics are gathered, which corresponds to the MIB node etherStatsDataSource.
etherStatsOctets	Number of octets received by the interface during the statistical period, corresponding to the MIB node etherStatsOctets.
etherStatsPkts	Number of packets received by the interface during the statistical period, corresponding to the MIB node etherStatsPkts.
etherStatsBroadcastPkts	Number of broadcast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsBroadcastPkts.
etherStatsMulticastPkts	Number of multicast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsMulticastPkts.
etherStatsUndersizePkts	Number of undersize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsUndersizePkts.
etherStatsOversizePkts	Number of oversize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsOversizePkts.
etherStatsFragments	Number of undersize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsFragments.
etherStatsJabbers	Number of oversize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsJabbers.
etherStatsCRCAlignErrors	Number of packets with CRC errors received on the interface during the statistical period, corresponding to the MIB node etherStatsCRCAlignErrors.
etherStatsCollisions	Number of collisions received on the interface during the statistical period, corresponding to the MIB node etherStatsCollisions.
etherStatsDropEvents	Total number of drop events received on the interface during the statistical period, corresponding to the MIB node etherStatsDropEvents.

Field	Description
Packets received according to length:	Incoming-packet statistics by packet length for the statistical period: • **64**—Number of 64-byte packets. The value is stored in the MIB node etherStatsPkts64Octets. • **65-127**—Number of 65- to 127-byte packets. The value is stored in the MIB node etherStatsPkts65to127Octets. • **128-255**—Number of 128- to 255-byte packets. to the value is stored in the MIB node etherStatsPkts128to255Octets. • **256-511**—Number of 256- to 511-byte packets. The value is stored in the MIB node etherStatsPkts256to511Octets. • **512-1023**—Number of 512- to 1023-byte packets. The value is stored in the MIB node etherStatsPkts512to1023Octets. • **1024-1518**—Number of 1024- to 1518-byte packets. The value is stored in the MIB node etherStatsPkts1024to1518Octets.

rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** \| **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the alarm entry index, which ranges from 1 to 65535.

alarm-variable: Specifies the alarm variable, a string of 1 to 256 characters. It can be in dotted object identifier (OID) format (in the format of *entry.integer.instance* or *leaf node name.instance*, for example, 1.3.6.1.2.1.2.1.10.1), or a node name like ifInOctets.1. Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument, such as the instance of the leaf node (like etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, and so on) of the etherStatsEntry entry, the instance of the leaf node (like ifInOctets, ifInUcastPkts, ifInNUcastPkts, and so on) of the ifEntry entry.

sampling-interval: Specifies the sampling interval, which ranges from 5 to 65535 seconds.

absolute: Sets the sampling type to **absolute**. In other words, the system obtains the value of the variable when the sampling time is reached.

delta: Sets the sampling type to **delta**. In other words, the system obtains the variation value of the variable during the sampling interval when the sampling time is reached.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range –2147483648 to +2147483647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range –2147483648 to +2147483647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65535. If 0 is specified, the alarm does not trigger any event.

owner *text*: Owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon alarm** to create an entry in the RMON alarm table.

Use **undo rmon alarm** to remove an entry from the RMON alarm table.

You can create up to 60 alarm entries.

To make sure that an alarm entry can take effect:

- Before creating an alarm entry, use the **rmon event** command to define the events to be referenced. Otherwise, the alarm entry cannot trigger events, even if it can be created.
- If the alarm variable is an instance of the leaf node of the Ethernet statistics table etherStatsEntry with the OID of 1.3.6.1.2.1.16.1.1.1, use the **rmon statistics** command to create a statistics entry on the monitored Ethernet interface. If the alarm variable is an instance of the leaf node of the history record table etherHistoryEntry with the OID of 1.3.6.1.2.1.16.2.2.1, use the **rmon history** command to create a history entry on the monitored Ethernet interface. Otherwise, the alarm entry cannot trigger events, even if it can be created.
- Make sure the alarm entry has different alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) than any existing alarm entry in the system.

When the alarm condition in an alarm entry occurs, its associated event is triggered to handle the alarm.

The system regularly samples the monitored alarm variables, compares the sampled values with the predefined thresholds, and does the following:

- If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
- If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

Related commands: **display rmon alarm**, **rmon event**, **rmon history**, and **rmon statistics**.

Examples

# Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Trigger event 1 when the sampled value is greater than or equal to the rising threshold of 5000, and event 2 when the sampled value is less than or equal to the falling threshold of 5. Set the owner of the entry to be **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

1.3.6.1.2.1.16.1.1.1.4 is the OID of the leaf node etherStatsOctets. It represents the statistics of the received packets on the interface, in bytes. In the above example, you can use etherStatsOctets.1 to replace the parameter 1.3.6.1.2.1.16.1.1.1.4.1, where 1 indicates the serial number of the interface statistics entry.

Therefore, if you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace the parameter.

This example enables the RMON agent to do the following:

- Samples and monitors interface GigabitEthernet 1/0/1.
- Obtains the incoming-packet count in its absolute value. If the total number of incoming bytes reaches 5000, the system logs the event. If the total number of incoming bytes is no more than 5, the system takes no action. To view the event log, use the **display rmon eventlog** command.

rmon event

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *log-trapcommunity* | **none** | **trap** *trap-community* } [**owner** *text*]

undo rmon event *entry-number*

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the event entry index, which ranges from 1 to 65535.

description *string*: Specifies the event description, a string of 1 to 127 characters.

log: Logs the event when it occurs.

log-trap *log-trapcommunity*: Specifies the log and trap events. The system performs both logging and trap sending when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

none: Performs no action when the event occurs.

trap *trap-community*: Specifies the trap event. The system sends a trap with a community name when the event occurs. *trap-community* specifies the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

owner *text*: Specifies the owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon event** to create an entry in the RMON event table.

Use **undo rmon event** to remove a specified entry from the RMON event table.

When creating an event entry, you can define the actions that the system takes when the event is triggered by its associated alarm in the alarm table. The system can log the event, send a trap, do both, or do neither based on your configuration.

An entry cannot be created if the values of the specified event description (**description** *string*), event type (**log**, **trap**, **logtrap** or **none**), and community name (*trap-community* or *log-trapcommunity)* to be identical to those of the existing event entry in the system.

Up to 60 event entries can be created.

Related commands: **display rmon event**, **rmon alarm**, and **rmon prialarm**.

Examples

# Create event 10 in the RMON event table.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

entry-number: Specifies the history control entry index, which ranges 1 to 65535.

buckets *number*: Specifies the history table size for the entry, which ranges from 1 to 65535.

interval *sampling-interval*: Specifies the sampling period, which ranges from 5 to 3600 seconds.

owner *text*: Specifies the owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon history** to create an entry in the RMON history control table.

Use **undo rmon history** to remove a specified entry from the RMON history control table.

After an entry is created, the system periodically samples the number of packets received/sent on the interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table. The maximum number of statistics records can be saved for the entry is specified by **buckets** *number*. If the maximum number of the statistics records for the entry has been reached, the system deletes the earliest record for the latest one. The statistics include total number of received packets on the interface, total number of broadcast packets, total number of multicast packets in a sampling period, and so on.

You can successfully create a history control entry, even if the specified bucket size exceeds the history table size supported by the device. However, the effective bucket size will be the actual value supported by the device. To view the configuration result, use the **display rmon history** command.

You can configure multiple history control entries for one interface, but must make sure their entry numbers and sampling intervals are different.

The device supports up to 100 history control entries.

Related commands: **display rmon history**.

Examples

# Create RMON history control entry 1 for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

rmon prialarm

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the index of a private alarm entry, which ranges from 1 to 65535.

prialarm-formula: Specifies the private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a point ".", the formula (.1.3.6.1.2.1.2.1.10.1)*8 for example. You can customize the formula and perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

prialarm-des: Specifies the private alarm entry description, a string of 1 to 127 characters.

sampling-interval: Specifies the sampling interval, which ranges from 10 to 65535 seconds.

absolute | **changeratio** | **delta**: Sets the sampling type to absolute, delta, or change ratio. Absolute sampling is to obtain the value of the variable when the sampling time is reached. Delta sampling is to obtain the variation value of the variable during the sampling interval when the sampling time is reached. Change ratio sampling is not supported at present.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range –2147483648 to +2147483647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65535, where 0 means no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range –2147483648 to +2147483647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65535.

forever: Indicates that the lifetime of the private alarm entry is infinite.

cycle *cycle-period*: Sets the lifetime period of the private alarm entry, which ranges from 0 to 2147483647 seconds.

owner *text*: Owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon prialarm** to create an entry in the private alarm table of RMON.

Use **undo rmon prialarm** to remove a private alarm entry from the private alarm table of RMON.

Before creating an alarm entry, use the **rmon event** command to define the events to be referenced in the event table.

You cannot create an entry that has the same alarm variable formula (*prialarm-formula*), sampling type (**absolute changeratio** or **delta**), rising threshold (*threshold-value1*), and falling threshold (*threshold-value2*) as an existing private alarm entry.

You can create up to 50 private alarm entries.

The system handles private alarm entries as follows:

1. Samples the private alarm variables in the private alarm formula at the specified sampling interval.
2. Performs calculation on the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds and does the following:
   - If the result is equal to or greater than the rising threshold, the system triggers the event specified by the *event-entry1* argument.
   - If the result is equal to or smaller than the falling threshold, the system triggers the event specified by the *event-entry2* argument.

Related commands: **display rmon prialarm**, **rmon event**, **rmon history**, and **rmon statistics**.

Examples

# Monitor the ratio of the broadcast packets received on the interface by using the private alarm.

Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1 * 100/.1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the variables at 10-second intervals. (Broadcast packet ratio= total number of broadcast packets received on the interface/total number of packets received on the interface; the formula is customized by users.)

The rising threshold (80%) triggers event 1 to log the event. The falling threshold (5%) triggers event 2, but the event defines neither log nor trap action.

Set the lifetime of the entry to **forever** and owner to **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfEth1/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the node etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the node etherStatsPkts.1. 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you should use 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5.

This example enables the RMON agent to do the following:

- Samples and monitors interface GigabitEthernet 1/0/1.
- If the portion of incoming broadcast packets in the total traffic crosses 80%, the system logs the event. If the portion is less than or equal to 5%, the system takes no action. To view the event log, use the **display rmon eventlog** command.

rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

entry-number: Specifies the index of statistics entry, which ranges from 1 to 65535.

owner *text*: Specifies the owner of the entry, a string of case-sensitive 1 to 127 characters that can contain spaces.

Description

Use **rmon statistics** to create an entry in the RMON statistics table.

Use **undo rmon statistics** to remove a specified entry from the RMON statistics table.

You can create one statistics entry for each interface, and up to 100 statistics entries on the device.

Each RMON statistics table entry provides a set of cumulative traffic statistics collected up to the present time for an interface. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, and number of packets received. The statistics are cleared at a reboot.

To display the RMON statistics table, use the **display rmon statistics** command.

Examples

# Create an entry with an index 20 and the owner **user1** in the RMON statistics table for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

Port mirroring configuration commands

display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

group-id: Number of the mirroring group to be displayed, ranging from 1 to 4.

all: Displays all mirroring groups.

local: Displays local mirroring groups.

remote-destination: Displays remote destination groups.

remote-source: Displays remote source groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mirroring-group** to display information about the specified mirroring groups, such as the types, status, and content of a mirroring group.

The output varies by mirroring group types and is sorted by mirroring group numbers.

Examples

# Display information about all the mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
        GigabitEthernet1/0/2  both
    monitor port: GigabitEthernet1/0/3
mirroring-group 2:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/0/4  both
    reflector port:
    monitor egress port: GigabitEthernet1/0/8
    remote-probe VLAN: 2
mirroring-group 3:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/7
    remote-probe VLAN: 3
```

Table 30 Command output

Field	Description
mirroring-group	Number of the mirroring group
type	Type of the mirroring group, which can be local, remote-source, or remote-destination
status	Status of the mirroring group, which can be active or inactive
mirroring port	Source port
monitor egress port	Egress port of a remote source group

mirroring-group

Syntax

mirroring-group *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View

System view

Default level

2: System level

Parameters

group-id: Specifies the number of the mirroring group to be created or removed, ranging from 1 to 4.

all: Removes all mirroring groups by using the **undo** command.

local: Creates a local mirroring group or removes all local mirroring groups with the **undo** command.

remote-destination: Creates a remote destination group or removes all remote destination groups with the **undo** command.

remote-source: Creates a remote source group or removes all remote source groups with the **undo** command.

Description

Use **mirroring-group** to create a mirroring group.

Use **undo mirroring-group** to remove the specified mirroring groups.

To mirror packets from a port to another port on the same device, create a local mirroring group.

To mirror packets from a port (a source port) on the current device to another port (the monitor port) either on the same device or on a different device, create remote mirroring groups. When doing that, create the remote source group on the device where the source port is located and create the remote destination group on the device where the monitor port is located.

By default, no mirroring group exists on a device.

Related commands: **sampler**.

Examples

# Create a local mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port

Syntax

mirroring-group *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

View

System view

Default level

2: System level

Parameters

group-id: Number of a local or remote source group, ranging from 1 to 4. The mirroring group specified by the *group-id* argument must already exist.

mirroring-port-list: A list of source ports/port ranges to be assigned to or removed from the mirroring group specified by *group-id*. You can specify up to eight single ports, port ranges, or combinations of both for the list. A single port takes the form of *interface-type interface-number*. A port range takes the form *interface-type interface-number* **to** *interface-type interface-number*, where the end port number must be greater than the start port number. For example, you may specify up to eight combinations of single ports and port ranges for the list like this: **gigabitethernet 1/0/1 gigabitethernet 1/0/3 gigabitethernet 1/0/5 gigabitethernet 2/0/2 to gigabitethernet 2/0/10 gigabitethernet 3/0/1 gigabitethernet 3/0/4 gigabitethernet 3/0/6 to gigabitethernet 3/0/10 gigabitethernet 3/0/12**.

both: Mirrors both inbound and outbound packets on the specified ports.

inbound: Mirrors only inbound packets on the specified ports.

outbound: Mirrors only outbound packets on the specified ports.

Description

Use **mirroring-group mirroring-port** to assign ports to a local or remote source group as source ports.

Use **undo mirroring-group mirroring-port** to remove source ports from the mirroring group.

By default, no source port is configured for any mirroring group.

You cannot configure source ports for a remote destination group.

When removing a source port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group mirroring-port** command matches the actual monitored direction specified earlier in the **mirroring-group mirroring-port** command.

Related commands: **mirroring-group**.

Examples

# Create local mirroring group 1, configure GigabitEthernet 1/0/1 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 both
```

# Create remote source group 2, configure GigabitEthernet 1/0/2 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] mirroring-group 2 mirroring-port GigabitEthernet 1/0/2 both
```

mirroring-group monitor-egress

Syntax

In system view:

mirroring-group *group-id* **monitor-egress** *monitor-egress-port*

undo mirroring-group *group-id* **monitor-egress** *monitor-egress-port*

In interface view:

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

View

System view, interface view

Default level

2: System level

Parameters

group-id: Number of a remote source group, ranging from 1 to 4. The mirroring group specified by *group-id* must already exist.

monitor-egress-port: Port to be configured as the egress port. It takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group monitor-egress** to configure a port as the egress port of a remote source group.

Use **undo mirroring-group monitor-egress** to remove the egress port of the mirroring group.

By default, no egress port is configured for a mirroring group.

You can configure an egress port only for a remote source group, not for other types of mirroring groups.

Related commands: **mirroring-group**.

Examples

# Create remote source group 1, and configure port GigabitEthernet 1/0/1 as its egress port in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress GigabitEthernet 1/0/1
```

# Create remote source group 2, and configure port GigabitEthernet 1/0/2 as its egress port in interface view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

mirroring-group monitor-port

Syntax

mirroring-group *group-id* **monitor-port** *monitor-port-id*

undo mirroring-group *group-id* **monitor-port** *monitor-port-id*

View

System view

Default level

2: System level

Parameters

group-id: Number of a local or remote destination group, ranging from 1 to 4. The mirroring group specified by *group-id* must already exist.

monitor-port-id: Port to be assigned to the specified mirroring group as the monitor port. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group monitor-port** to assign a port to a local or remote destination group as the monitor port.

Use **undo mirroring-group monitor-port** to remove the monitor port from the local or remote destination group.

By default, no monitor port is configured for a mirroring group.

You cannot configure a monitor port for a remote source group.

You cannot assign a source port in an existing mirroring group to another mirroring group as the monitor port.

Related commands: **mirroring-group**.

Examples

# Create local mirroring group 1, and configure port GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

```
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/1
```

# Create remote destination group 2, and configure port GigabitEthernet 1/0/2 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 monitor-port GigabitEthernet 1/0/2
```

mirroring-group reflector-port

Syntax

In system view:

mirroring-group *group-id* **reflector-port** *reflector-port*

undo mirroring-group *group-id* **reflector-port** *reflector-port*

In interface view:

mirroring-group *group-id* **reflector-port**

undo mirroring-group *group-id* **reflector-port**

View

System view, interface view

Default level

2: System level

Parameters

group-id: Number of a remote source group, ranging from 1 to 4. The mirroring group specified by *group-id* must already exist.

reflector-port: Port to be configured as the reflector port in the specified mirroring group. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group reflector-port** to configure the reflector port in a remote source group.

Use **undo mirroring-group reflector-port** to remove the reflector port of the remote source group.

By default, no reflector port is configured for a mirroring group, and a port does not serve as the reflector port of any mirroring group.

You can configure a reflector port for a remote source group only, not for other types of mirroring groups.

Related commands: **mirroring-group**.

Examples

# Create remote source group 1, and configure port GigabitEthernet 1/0/1 as its reflector port in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 reflector-port GigabitEthernet 1/0/1
```

# Create remote source group 2, and configure port GigabitEthernet 1/0/2 as its reflector port in interface view.

```
<Sysname> system-view
```

```
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 reflector-port
```

mirroring-group remote-probe vlan

Syntax

mirroring-group *group-id* **remote-probe vlan** *rprobe-vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *rprobe-vlan-id*

View

System view

Default level

2: System level

Parameters

group-id: Number of a remote source or destination mirroring group, ranging from 1 to 4. The mirroring group specified by *group-id* must already exist.

rprobe-vlan-id: ID of the VLAN to be configured as the remote probe VLAN. This VLAN must be a static VLAN that already exists.

Description

Use **mirroring-group remote-probe vlan** to specify a VLAN as the remote probe VLAN for a remote source or destination mirroring group.

Use **undo mirroring-group remote-probe vlan** to remove the remote probe VLAN from the remote source or destination mirroring group.

By default, no remote probe VLAN is configured for a mirroring group.

For a remote source or destination mirroring group, you must configure and can configure only one remote probe VLAN to carry mirrored packets. You cannot configure the remote probe VLAN for a local mirroring group.

Only a static VLAN that already exists can be configured as a remote probe VLAN; a VLAN can serve as the remote probe VLAN of only one mirroring group.

To delete a VLAN that is configured as a remote probe VLAN, remove the remote probe VLAN configuration first.

Related commands: **mirroring-group**.

Examples

# Create remote source group 1, and configure VLAN 10 as its remote probe VLAN.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 10
```

# Create remote destination group 2, and configure VLAN 20 as its remote probe VLAN.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 remote-probe vlan 20
```

mirroring-port

Syntax

[**mirroring-group** *group-id*] **mirroring-port** { **inbound** | **outbound** | **both** }

undo [**mirroring-group** *group-id*] **mirroring-port** { **inbound** | **outbound** | **both** }

View

Interface view

Default level

2: System level

Parameters

mirroring-group *group-id*: Specifies a local or remote source group by its number, which ranges from 1 to 4 and defaults to 1. The mirroring group specified by *group-id* must already exist.

both: Mirrors both inbound and outbound packets on the current port.

inbound: Mirrors only inbound packets on the current port.

outbound: Mirrors only outbound packets on the current port.

Description

Use **mirroring-port** to assign the current port to a local or remote source group as a source port.

Use **undo mirroring-port** to remove the current port from the mirroring group.

By default, a port does not serve as a source port for any mirroring group.

You cannot configure source ports for a remote destination group.

When removing a source port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group** command matches the actual monitored direction of the port specified earlier in the **mirroring-port** command.

Examples

# Create local mirroring group 1, configure GigabitEthernet 1/0/1 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both
```

# Create remote source group 2, configure GigabitEthernet 1/0/2 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 mirroring-port both
```

monitor-port

Syntax

[**mirroring-group** *group-id*] **monitor-port**

undo [**mirroring-group** *group-id*] **monitor-port**

View

Interface view

Default level

2: System level

Parameters

mirroring-group *group-id*: Specifies a local or remote destination group by its number, which ranges from 1 to 4 and defaults to 1. The mirroring group specified by *group-id* must already exist.

Description

Use **monitor-port** to assign the current port to a local or remote destination group as the monitor port.

Use **undo monitor-port** to remove the current port from the mirroring group.

By default, a port does not serve any mirroring group as the monitor port.

You cannot configure a monitor port for a remote source group.

You cannot configure a source port of an existing mirroring group as a monitor port.

Related commands: **mirroring-group**.

Examples

# Create local mirroring group 1, and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] monitor-port
```

# Create remote destination group 2, and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] monitor-port
```

Traffic mirroring configuration commands

The traffic mirroring and remote traffic mirroring functions on the switch are implemented through the cooperation of a QoS policy and remote port mirroring. For the configuration commands about a QoS policy, see *ACL and QoS Command Reference*.

mirror-to

Syntax

mirror-to { **cpu** | **interface** *interface-type interface-number* }

undo mirror-to { **cpu** | **interface** *interface-type interface-number* }

View

Traffic behavior view

Default level

2: System level

Parameters

cpu: Mirrors traffic to the CPU, which is the CPU of the device where ports with traffic mirroring configured resides.

interface *interface-type interface-number*: Mirrors traffic to a port specified by its type and number.

Description

Use **mirror-to** to configure traffic mirroring for a traffic behavior.

Use **undo mirror-to** to remove traffic mirroring configuration.

By default, traffic mirroring is not configured for a traffic behavior.

You can configure the action of mirroring traffic to a port multiple times for a traffic behavior. Traffic can only be mirrored to the CPU or a port in a traffic behavior.

Examples

# Create traffic behavior 1 and configure the action of mirroring traffic to the CPU for the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to cpu
```

# Create traffic behavior 1 and configure the action of mirroring traffic to port GigabitEthernet 1/0/1 for the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface GigabitEthernet 1/0/1
```

NQA configuration commands

NQA client configuration commands

advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

View

Voice test type view

Default level

2: System level

Parameters

factor: Specifies the advantage factor, used to count Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values. The value is in the range of 0 to 20.

Description

Use **advantage-factor** to configure the advantage factor that is used to count MOS and ICPIF values.

Use **undo advantage-factor** to restore the default.

By default, the advantage factor is 0.

The evaluation of voice quality depends on users' tolerance for voice quality, and this factor should be taken into consideration. For users with higher tolerance for voice quality, use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values and both the objective and subjective factors are considered when you evaluate voice quality.

Examples

# Configure the advantage factor for a voice test as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

View

Voice test type view

Default level

2: System level

Parameters

g711a: Specifies a G.711 A-law codec type.

g711u: Specifies a G.711 *μ*-law codec type

g729a: Specifies a G.729 A-law codec type.

Description

Use **codec-type** to configure the codec type for a voice test.

Use **undo codec-type** to restore the default.

By default, the codec type for a voice test is G.711 A-law.

Examples

# Configure the codec type for a voice test as **g729a**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

data-fill

Syntax

data-fill *string*

undo data-fill

View

ICMP echo, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

string: Specifies a case-sensitive string of 1 to 200 characters.

Description

Use **data-fill** to configure the string to be filled in the data field of a probe packet.

Use **undo data-fill** to restore the default.

By default, the string is the hexadecimal number 00010203040506070809.

- If the data field length is smaller than the string length, only the first part of the string is filled. For example, if you configure the string as **abcd** and the data field size as 3 bytes, **abc** is filled.
- If the data field length is greater than the string length, the system fills the data field with the string cyclically until the data field is full. For example, if you configure the string as **abcd** and the data field size as 6 bytes, **abcdab** is filled.

How the string is filled varies with test types:

- For ICMP echo tests, the string fills the whole data field of ICMP echo requests.
- For UDP echo tests, the first five bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of data field.
- For UDP jitter tests, the first 68 bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of the data field.
- For voice tests, the first 16 bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of the data field.

Examples

# Configure string **abcd** to be filled in the data field of an ICMP echo request.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

data-size

Syntax

data-size *size*

undo data-size

View

ICMP echo, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

size: Specifies the size of the data field in a probe packet in bytes. The value is in the range of 20 to 8100 for probe packets of ICMP echo or UDP echo tests, 68 to 8100 for probe packets of UDP jitter tests, and 16 to 1500 for probe packets of voice tests.

Description

Use **data-size** to configure the size of the data field in each ICMP echo request of the ICMP echo tests or in each UDP packet of UDP echo, UDP jitter, or voice tests.

Use **undo data-size** to restore the default.

Table 31 Default values of the size of a probe packet

Test type	Codec type	Default value (in bytes)
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

Examples

# Configure the size of the data field in an ICMP echo request as 80 bytes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

description (any NQA test type view)

Syntax

description *text*

undo description

View

Any NQA test type view

Default level

2: System level

Parameters

text: Specifies a case-sensitive string of 1 to 200 characters, used to describe a test group.

Description

Use **description** to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use **undo description** to remove the configured description information.

By default, no descriptive string is available for a test group.

Examples

# Configure the descriptive string for a test group as **icmp-probe**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

destination ip

Syntax

destination ip *ip-address*

undo destination ip

View

DLSw, FTP, DNS, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

ip-address: Specifies the destination IP address of a test operation.

Description

Use **destination ip** to configure a destination IP address for a test operation.

Use **undo destination ip** to remove the configured destination IP address.

By default, no destination IP address is configured for a test operation.

Examples

# Configure the destination IP address of an ICMP echo test operation as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

destination port

Syntax

destination port *port-number*

undo destination port

View

TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

port-number: Specifies the destination port number of a test operation, in the range of 1 to 65535.

Description

Use **destination port** to configure a destination port number for a test operation.

Use **undo destination port** to remove the configured destination port number.

By default, no destination port number is configured for a test operation.

Do not perform a UDP jitter test and a voice test on ports from 1 to 1023 (known ports). Otherwise, the NQA test fails or the corresponding services of this port are unavailable.

Examples

# Configure the destination port number of a test operation as 9000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

display nqa history

Syntax

display nqa history [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays history records of an NQA test group. If these two arguments are not specified, history records of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation. It is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag. It is a case-insensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display nqa history** to display history records of the specified or all NQA test groups.

The **display nqa history** command cannot show you the results of voice tests and UDP jitter tests. To know the result of a voice test or a UDP jitter test, use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

Examples

# Display the history records of the NQA test group in which the administrator name is **administrator**, and the operation tag is **test**.

```
<Sysname> display nqa history administrator test
  NQA entry (admin administrator, tag test) history record(s):
    Index      Response     Status           Time
    10         329          Succeeded        2011-01-23 20:54:26.5
    9          344          Succeeded        2011-01-23 20:54:26.2
    8          328          Succeeded        2011-01-23 20:54:25.8
    7          328          Succeeded        2011-01-23 20:54:25.5
    6          328          Succeeded        2011-01-23 20:54:25.1
    5          328          Succeeded        2011-01-23 20:54:24.8
    4          328          Succeeded        2011-01-23 20:54:24.5
    3          328          Succeeded        2011-01-23 20:54:24.1
    2          328          Succeeded        2011-01-23 20:54:23.8
    1          328          Succeeded        2011-01-23 20:54:23.4
```

Table 32 Command output

Field	Description
Index	History record number
Response	Round-trip delay of a test packet in the case of a successful test, timeout time in the case of timeout, or 0 in the case that a test cannot be completed (in milliseconds)

Field	Description
Status	Status value of test results, which can be one of the following values: • Succeeded • Unknown error • Internal error • Timeout
Time	Time when the test is completed

display nqa reaction counters

Syntax

display nqa reaction counters [*admin-name operation-tag* [*item-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays current monitoring results of reaction entries in a test group. If these two arguments are not specified, monitoring results of all reaction entries of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation. It is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag. It is a case-insensitive string of 1 to 32 characters.

item-number: Displays current monitoring results of a specific reaction entry. If this argument is not provided, results of all reaction entries are displayed. *item-number* represents the reaction entry ID, in the range of 1 to 10.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display nqa reaction counters** to display the current monitoring results of reaction entries.

If the threshold type is average value, or the monitored element is ICPIF or MOS in a voice test, the monitoring results are invalid.

The monitoring results are accumulated since the test group starts and are not cleared after the test completes.

Examples

# Display the monitoring results of all reaction entries in an ICMP echo test group, in which the administrator name is **admin**, and the operation tag is **test**.

```
<Sysname> display nqa reaction counters admin test
  NQA entry (admin admin, tag test) reaction counters:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      probe-duration   accumulate      12           4
    2      probe-duration   average         -            -
    3      probe-duration   consecutive     160          56
    4      probe-fail       accumulate      12           0
    5      probe-fail       consecutive     162          2
```

Table 33 Command output

Field	Description
Index	ID of a reaction entry
Checked Element	Monitored element
Threshold Type	Threshold type
Checked Num	Number of targets that have been monitored for data collection
Over-threshold Num	Number of threshold violations

Table 34 Description on the threshold monitoring fields of the display nqa reaction counters command

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes since the group starts	Number of finished probes since the test group starts	Number of probes of which the duration exceeds the threshold since the test group starts
	average	N/A	N/A	N/A
	consecutive	Probes since the test group starts	Number of finished probes since the test group starts	Number of probes of which the duration exceeds the threshold since the test group starts
probe-fail	accumulate	Probes since the test group starts	Number of finished probes since the test group starts	Number of probe failures since the test group starts
	consecutive	Probes since the test group starts	Number of finished probes since the test group starts	Number of probe failures since the test group starts
RTT	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the round-trip time exceeds the threshold since the test group starts
	average	N/A	N/A	N/A

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
jitter-DS/jitter-SD	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the one-way delay jitter exceeds the threshold since the test group starts
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the one-way delay exceeds the threshold since the test group starts
packet-loss	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Total packet loss since the test group starts
ICPIF	N/A	N/A	N/A	N/A
MOS	N/A	N/A	N/A	N/A

display nqa result

Syntax

display nqa result [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays results of the last test of a test group. If these two arguments are not specified, results of the last tests of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation, and it is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag, and it is a case-insensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display nqa result** to display results of the last NQA test.

Examples

# Display the results of the last UDP jitter test.

```
<Sysname> display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 192.168.1.42
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 15/46/26
      Square-Sum of round trip time: 8103
      Last succeeded probe time: 2011-01-23 10:56:38.7
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 10
      Min positive SD: 8                     Min positive DS: 8
      Max positive SD: 18                    Max positive DS: 8
      Positive SD number: 5                  Positive DS number: 2
      Positive SD sum: 75                    Positive DS sum: 32
      Positive SD average: 15                Positive DS average: 16
      Positive SD square sum: 1189           Positive DS square sum: 640
      Min negative SD: 8                     Min negative DS: 1
      Max negative SD: 24                    Max negative DS: 30
      Negative SD number: 4                  Negative DS number: 7
      Negative SD sum: 56                    Negative DS sum: 99
      Negative SD average: 14                Negative DS average: 14
      Negative SD square sum: 946            Negative DS square sum: 1495
    One way results:
      Max SD delay: 22                       Max DS delay: 23
      Min SD delay: 7                        Min DS delay: 7
      Number of SD delay: 10                 Number of DS delay: 10
      Sum of SD delay: 125                   Sum of DS delay: 132
      Square sum of SD delay: 1805           Square sum of DS delay: 1988
      SD lost packet(s): 0                   DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
```

# Display the results of the last voice test.

```
<Sysname> display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 192.168.1.42
      Send operation times: 1000           Receive response times: 0
      Min/Max/Average round trip time: 0/0/0
      Square-Sum of round trip time: 0
      Last succeeded probe time: 0-00-00 00:00:00.0
    Extended results:
      Packet loss in test: 100%
      Failures due to timeout: 1000
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 0
      Min positive SD: 0                     Min positive DS: 0
      Max positive SD: 0                     Max positive DS: 0
      Positive SD number: 0                  Positive DS number: 0
      Positive SD sum: 0                     Positive DS sum: 0
      Positive SD average: 0                 Positive DS average: 0
      Positive SD square sum: 0              Positive DS square sum: 0
      Min negative SD: 0                     Min negative DS: 0
      Max negative SD: 0                     Max negative DS: 0
      Negative SD number: 0                  Negative DS number: 0
      Negative SD sum: 0                     Negative DS sum: 0
      Negative SD average: 0                 Negative DS average: 0
      Negative SD square sum: 0              Negative DS square sum: 0
    One way results:
      Max SD delay: 0                        Max DS delay: 0
      Min SD delay: 0                        Min DS delay: 0
      Number of SD delay: 0                  Number of DS delay: 0
      Sum of SD delay: 0                     Sum of DS delay: 0
      Square sum of SD delay: 0              Square sum of DS delay: 0
      SD lost packet(s): 0                   DS lost packet(s): 0
      Lost packet(s) for unknown reason: 1000
    Voice scores:
      MOS value: 0.99                        ICPIF value: 87
```

Table 35 Command output

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds
Square-Sum of round trip time	Square sum of round-trip time
Last succeeded probe time	Time when the last successful probe was finished
Packet loss in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures due to out-of-sequence packets

Field	Description
Failures due to internal error	Number of failures due to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of packets that arrived late
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests
Voice results	Voice test results, available only in voice tests
RTT number	Number of response packets received
Min positive SD	Minimum positive delay jitters from source to destination
Min positive DS	Minimum positive delay jitters from destination to source
Max positive SD	Maximum positive delay jitters from source to destination
Max positive DS	Maximum positive delay jitters from destination to source
Positive SD number	Number of positive delay jitters from source to destination
Positive DS number	Number of positive delay jitters from destination to source
Positive SD sum	Sum of positive delay jitter from source to destination
Positive DS sum	Sum of positive delay jitters from destination to source
Positive SD average	Average of positive delay jitter from source to destination
Positive DS average	Average of positive delay jitter from destination to source
Positive SD square sum	Square sum of positive delay jitters from source to destination
Positive DS square sum	Square sum of positive delay jitters from destination to source
Min negative SD	Minimum absolute value among negative delay jitters from source to destination
Min negative DS	Minimum absolute value among negative delay jitters from destination to source
Max negative SD	Maximum absolute value among negative delay jitters from source to destination
Max negative DS	Maximum absolute value among negative delay jitters from destination to source
Negative SD number	Number of negative delay jitters from source to destination
Negative DS number	Number of negative delay jitters from destination to source
Negative SD sum	Sum of absolute values of negative delay jitters from source to destination
Negative DS sum	Sum of absolute values of negative delay jitters from destination to source
Negative SD average	Average absolute value of negative delay jitters from source to destination
Negative DS average	Average absolute value of negative delay jitters from destination to source
Negative SD square sum	Square sum of negative delay jitters from source to destination
Negative DS square sum	Square sum of negative delay jitters from destination to source

Field	Description
One way results	Uni-direction delay test result, displayed in a UDP jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
MOS value	MOS value calculated for a voice test
ICPIF value	ICPIF value calculated for a voice test

display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays statistics of the specified test group. If these two arguments are not specified, statistics of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation, and it is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag, and it is a case-insensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display nqa statistics** to display test result statistics for the specified or all test groups.

Statistics cannot be generated until all probe operations in the first test of a test group have finished. If they have not finished and you display statistics by using this command, the statistics are display as all 0s.

If a reaction entry is configured, the command displays the monitoring results of the reaction entry in the period specified by the **statistics internal** command. If the threshold type is average value or the monitored element is ICPIF or MOS for voice tests, the monitoring results are invalid.

Related commands: **statistics interval**.

Examples

# Display statistics of UDP jitter tests.

```
<Sysname> display nqa statistics admin test
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 1.1.1.2
      Start time: 2011-01-01 09:33:22.3
      Life time: 23 seconds
      Send operation times: 100            Receive response times: 100
      Min/Max/Average round trip time: 1/11/5
      Square-Sum of round trip time: 24360
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 550
      Min positive SD: 1                     Min positive DS: 1
      Max positive SD: 7                     Max positive DS: 1
      Positive SD number: 220                Positive DS number: 97
      Positive SD sum: 283                   Positive DS sum: 287
      Positive SD average: 1                 Positive DS average: 2
      Positive SD square sum: 709            Positive DS square sum: 1937
      Min negative SD: 2                     Min negative DS: 1
      Max negative SD: 10                    Max negative DS: 1
      Negative SD number: 81                 Negative DS number: 94
      Negative SD sum: 556                   Negative DS sum: 191
      Negative SD average: 6                 Negative DS average: 2
      Negative SD square sum: 4292           Negative DS square sum: 967
    One way results:
      Max SD delay: 5                        Max DS delay: 5
      Min SD delay: 1                        Min DS delay: 1
      Number of SD delay: 550                Number of DS delay: 550
      Sum of SD delay: 1475                  Sum of DS delay: 1201
      Square sum of SD delay: 5407           Square sum of DS delay: 3959
      SD lost packet(s): 0                   DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
    Reaction statistics:
      Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
      1      jitter-DS        accumulate      90           25
      2      jitter-SD        average         -            -
      3      OWD-DS           -               100          24
      4      OWD-SD           -               100          13
      5      packet-loss      accumulate      0            0
      6      RTT              accumulate      100          52
```

# Display statistics of voice tests.

```
<Sysname> display nqa statistics admin test
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 1.1.1.2
      Start time: 2011-01-01 09:33:45.3
      Life time: 120 seconds
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 1/12/7
      Square-Sum of round trip time: 620
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 10
      Min positive SD: 3                     Min positive DS: 1
      Max positive SD: 10                    Max positive DS: 1
      Positive SD number: 3                  Positive DS number: 2
      Positive SD sum: 18                    Positive DS sum: 2
      Positive SD average: 6                 Positive DS average: 1
      Positive SD square sum: 134            Positive DS square sum: 2
      Min negative SD: 3                     Min negative DS: 1
      Max negative SD: 9                     Max negative DS: 1
      Negative SD number: 4                  Negative DS number: 2
      Negative SD sum: 25                    Negative DS sum: 2
      Negative SD average: 6                 Negative DS average: 1
      Negative SD square sum: 187            Negative DS square sum: 2
    One way results:
```

```
    Max SD delay: 0                         Max DS delay: 0
    Min SD delay: 0                         Min DS delay: 0
    Number of SD delay: 0                   Number of DS delay: 0
    Sum of SD delay: 0                      Sum of DS delay: 0
    Square sum of SD delay: 0               Square sum of DS delay: 0
    SD lost packet(s): 0                    DS lost packet(s): 0
    Lost packet(s) for unknown reason: 0
  Voice scores:
    Max MOS value: 4.40                     Min MOS value: 4.40
    Max ICPIF value: 0                      Min ICPIF value: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      ICPIF            -               -            -
    2      MOS              -               -            -
```

Table 36 Command output

Field	Description
No.	Statistics group number
Destination IP address	IP address of the destination
Start time	Time when the test group starts
Life time	Duration of the test, in seconds
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds
Square-Sum of round trip time	Square sum of round-trip time
Packet loss in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures due to out-of-sequence packets
Failures due to internal error	Number of failures due to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of response packets received after a probe times out
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests
Voice results	Voice test results, available only in voice tests
RTT number	Number of response packets received
Min positive SD	Minimum positive delay jitter from source to destination
Min positive DS	Minimum positive delay jitter from destination to source
Max positive SD	Maximum positive delay jitter from source to destination
Max positive DS	Maximum positive delay jitter from destination to source
Positive SD number	Number of positive delay jitters from source to destination

Field	Description
Positive DS number	Number of positive delay jitters from destination to source
Positive SD sum	Sum of positive delay jitters from source to destination
Positive DS sum	Sum of positive delay jitters from destination to source
Positive SD average	Average of positive delay jitters from source to destination
Positive DS average	Average of positive delay jitters from destination to source
Positive SD square sum	Square sum of positive delay jitters from source to destination
Positive DS square sum	Square sum of positive delay jitters from destination to source
Min negative SD	Minimum absolute value among negative delay jitters from source to destination
Min negative DS	Minimum absolute value among negative delay jitters from destination to source
Max negative SD	Maximum absolute value among negative delay jitters from source to destination
Max negative DS	Maximum absolute value among negative delay jitters from destination to source
Negative SD number	Number of negative delay jitters from source to destination
Negative DS number	Number of negative delay jitters from destination to source
Negative SD sum	Sum of absolute values of negative delay jitters from source to destination
Negative DS sum	Sum of absolute values of negative delay jitters from destination to source
Negative SD average	Average absolute value of negative delay jitters from source to destination
Negative DS average	Average absolute value of negative delay jitters from destination to source
Negative SD square sum	Square sum of negative delay jitters from source to destination
Negative DS square sum	Square sum of negative delay jitters from destination to source
One way results	Uni-direction delay test result, displayed on in a UDP Jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source

Field	Description
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
Max MOS value	Maximum MOS value
Min MOS value	Minimum MOS value
Max ICPIF value	Maximum ICPIF value
Min ICPIF value	Minimum ICPIF value
Reaction statistics	Statistics about the reaction entry in the counting interval
Index	ID of a reaction entry
Checked Element	Monitored element
Threshold Type	Threshold type
Checked Num	Number of targets that have been monitored for data collection
Over-threshold Num	Number of threshold violations

Table 37 Description on the threshold monitoring fields of the display nqa statistics command

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes in the counting interval	Number of finished probes in the counting interval	Number of probes of which the duration exceeds the threshold in the counting interval
	average	N/A	N/A	N/A
	consecutive	Probes in the counting interval	Number of finished probes in the counting interval	Number of probes of which the duration exceeds the threshold in the counting interval
probe-fail	accumulate	Probes in the counting interval	Number of finished probes in the counting interval	Number of probe failures in the counting interval
	consecutive	Probes in the counting interval	Number of finished probes in the counting interval	Number of probe failures in the counting interval
RTT	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the round-trip time exceeds the threshold in the counting interval
	average	N/A	N/A	N/A

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
jitter-DS/jitter-SD	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the one-way delay jitter exceeds the threshold in the counting interval
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the one-way delay exceeds the threshold in the counting interval
packet-loss	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packet loss in the counting interval
ICPIF	N/A	N/A	N/A	N/A
MOS	N/A	N/A	N/A	N/A

filename

Syntax

filename *filename*

undo filename

View

FTP test type view

Default level

2: System level

Parameters

filename: Specifies the name of the file transferred between the FTP server and the FTP client. The file name is a case-sensitive string of 1 to 200 characters.

Description

Use **filename** to specify a file to be transferred between the FTP server and the FTP client.

Use **undo filename** to restore the default.

By default, no file is specified.

Examples

# Specify the file to be transferred between the FTP server and the FTP client as **config.txt**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

frequency

Syntax

frequency *interval*

undo frequency

View

Any NQA test type view

Default level

2: System level

Parameters

interval: Specifies the interval in milliseconds between two consecutive tests, in the range of 0 to 604800000. The value 0 sets the test group to perform only one test, and not to collect any statistics.

Description

Use **frequency** to configure the interval between two consecutive tests for a test group. When a test group starts, it performs tests one by one at the specified interval. However, if a test is not completed when the interval is reached, no new test starts.

Use **undo frequency** to restore the default.

By default, the interval between two consecutive voice tests is 60000 milliseconds, and the interval between two consecutive tests of other types is 0 milliseconds.

Examples

# Configure the ICMP echo test group starts tests one by one at an interval of 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

history-record enable

Syntax

history-record enable

undo history-record enable

View

Any NQA test type view

Default level

2: System level

Parameters

None

Description

Use **history-record enable** to enable the saving of history records of an NQA test group.

Use **undo history-record enable** to disable the history records saving function.

By default, history records of an NQA test group are not saved.

If the history records saving function is enabled, the system saves the history records. To view the history records of the NQA test group, use the **display nqa history** command.

If the history records saving function is disabled, the system does not save the history records of the NQA test group and the existing history records are also removed.

Related commands: **display nqa history**.

Examples

# Enable the history records saving function of an NQA test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record enable
```

history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

View

Any NQA test type view

Default level

2: System level

Parameters

keep-time: Specifies how long the history records can be saved. The time is in the range of 1 to 1440 minutes.

Description

Use **history-record keep-time** to set the lifetime of the history records in an NQA test group.

Use **undo history-record keep-time** to restore the default.

By default, the history records in an NQA test group are kept for 120 minutes.

When an NQA test completes, the timing starts. All the records are removed when the lifetime is reached.

Examples

# Configure the lifetime of the history records in an NQA test group as 100 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record keep-time 100
```

history-record number

Syntax

history-record number *number*

undo history-record number

View

Any NQA test type view

Default level

2: System level

Parameters

number: Specifies the maximum number of history records that can be saved in a test group. The value is in the range of 0 to 50.

Description

Use **history-record number** to configure the maximum number of history records that can be saved in a test group.

Use **undo history-record number** to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the number of history records in a test group exceeds the maximum number, the earliest history record is removed.

Examples

# Configure the maximum number of history records that can be saved in a test group as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record number 10
```

http-version

Syntax

http-version v1.0

undo http-version

View

HTTP test type view

Default level

2: System level

Parameters

v1.0: Uses HTTP version 1.0 in an HTTP test.

Description

Use **http-version** to configure the HTTP version used in an HTTP test.

Use **undo http-version** to restore the default.

By default, HTTP 1.0 is used in an HTTP test.

Examples

# Configure the HTTP version as 1.0 in an HTTP test.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] http-version v1.0
```

mode

Syntax

mode { **active** | **passive** }

undo mode

View

FTP test type view

Default level

2: System level

Parameters

active: Sets the data transmission mode to active for FTP tests. In this mode, the FTP server initiates a data connection request.

passive: Sets the data transmission mode to passive for FTP tests. In this mode, a client initiates a data connection request.

Description

Use **mode** to set the data transmission mode for FTP tests.

Use **undo mode** to restore the default.

By default, the data transmission mode is **active**.

Examples

# Set the data transmission mode to passive for FTP tests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] mode passive
```

next-hop

Syntax

next-hop *ip-address*

undo next-hop

View

ICMP echo test type view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of the next hop.

Description

Use **next-hop** to configure the next hop IP address for ICMP echo requests of a test group.

Use **undo next-hop** to remove the configured next hop IP address.

By default, no next hop IP address is configured.

Examples

# Configure the next hop IP address as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop 10.1.1.1
```

nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

View

System view

Default level

2: System level

Parameters

admin-name: Specifies the name of the NQA test group administrator who creates the NQA test operation, a case-insensitive string of 1 to 32 characters, with "-" excluded.

operation-tag: Specifies the tag of a test operation, a case-insensitive string of 1 to 32 characters, with "-" excluded.

all: Removes all NQA test groups.

Description

Use **nqa** to create an NQA test group and enter NQA test group view.

Use **undo nqa** to remove the test group.

If the test type has been configured for the test group, you directly enter NQA test type view when you execute the **nqa** command.

Examples

# Create an NQA test group whose administrator name is **admin** and whose operation tag is **test** and enter NQA test group view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **nqa agent enable** to enable the NQA client.

Use **undo nqa agent enable** to disable the NQA client and stop all the tests being performed.

By default, the NQA client is enabled.

Related commands: **nqa server enable**.

Examples

# Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa agent enable
```

nqa agent max-concurrent

Syntax

nqa agent max-concurrent *number*

undo nqa agent max-concurrent

View

System view

Default level

2: System level

Parameters

number: Specifies the maximum number of tests that the NQA client can simultaneously perform. The value is in the range of 1 to 30.

Description

Use **nqa agent max-concurrent** to configure the maximum number of tests that the NQA client can simultaneously perform.

Use **undo nqa agent max-concurrent** to restore the default.

By default, the maximum number is 2.

From the beginning to the end of a test, the NQA test is in test status; from the end of a test to the beginning of the next test, the NQA test is in waiting status.

Examples

# Configure the maximum number of tests that the NQA client can simultaneously perform as 5.

```
<Sysname> system-view
[Sysname] nqa agent max-concurrent 5
```

nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh*:*mm*:*ss* [*yyyy/mm/dd*] | **now** } **lifetime** { *lifetime* | **forever** }

undo nqa schedule *admin-name operation-tag*

View

System view

Default level

2: System level

Parameters

admin-name: Specifies the name of the NQA test group administrator who creates the NQA test operation. The name is a case-insensitive string of 1 to 32 characters.

operation-tag: Specifies the test operation tag, a case-insensitive string of 1 to 32 characters.

start-time: Specifies the start time and date of a test group.

hh:*mm*:*ss*: Specifies the start time of a test group.

yyyy/mm/dd: Specifies the start date of a test group. The default value is the current system time, and *yyyy* is in the range of 2000 to 2035.

now: Starts the tests for a test group immediately.

lifetime: Specifies the duration of the test operation.

lifetime: Specifies the duration of the test operation in seconds, in the range of 1 to 2147483647.

forever: Specifies that the tests are performed for a test group forever.

Description

Use **nqa schedule** to configure the test start time and test duration for a test group.

Use **undo nqa schedule** to stop the test for the test group.

You cannot enter test group view or test type view after a test group is scheduled.

A test group performs a test when the system time is between the start time and the end time (the start time plus test duration). If the system time is behind the start time when you execute the **nqa schedule** command, a test is started when the system time reaches the start time; if the system time is between the start time and the end time, a test is started immediately; if the system time is ahead of the end time, no test is started. To view the current system time, use the **display clock** command.

Related commands: **display clock** (*Fundamentals Command Reference*).

Examples

# Start the tests for the test group with the administrator name **admin** and operation tag **test**. The start time and duration of the test group are 08:08:08 2011/01/08 and 1000 seconds.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time 08:08:08 2011/01/08 lifetime 1000
```

operation (FTP test type view)

Syntax

operation { **get** | **put** }

undo operation

View

FTP test type view

Default level

2: System level

Parameters

get: Obtains a file from the FTP server.

put: Transfers a file to the FTP server.

Description

Use **operation** to configure the FTP operation type.

Use **undo operation** to restore the default.

By default, the FTP operation type is **get**.

Examples

# Configure the FTP operation type as **put**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

operation (HTTP test type view)

Syntax

operation { **get** | **post** }

undo operation

View

HTTP test type view

Default level

2: System level

Parameters

get: Obtains data from the HTTP server.

post: Transfers data to the HTTP server.

Description

Use **operation** to configure the HTTP operation type.

Use **undo operation** to restore the default.

By default, the HTTP operation type is **get**.

Examples

# Configure the HTTP operation type as **post**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation post
```

operation interface

Syntax

operation interface *interface-type interface-number*

undo operation interface

View

DHCP test type view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **operation interface** to specify the interface to perform a DHCP test. The specified interface must be up; otherwise, no probe packets can be sent out.

Use **undo operation interface** to restore the default.

By default, no interface is specified to perform a DHCP test.

Examples

# Specify the interface to perform a DHCP test as VLAN-interface 2.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

password (FTP test type view)

Syntax

password [**cipher** | **simple**] *password*

undo password

View

FTP test type view

Default level

2: System level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies a password used to log in to the FTP server. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Description

Use **password** to configure a password used to log onto the FTP server.

Use **undo password** to remove the configured password.

By default, no password is configured for logging onto the FTP server.

The password set in either plaintext or ciphertext is saved in ciphertext in the configuration file.

Related commands: **username** and **operation**.

Examples

# Configure the password used for logging in to the FTP server as **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password ftpuser
```

probe count

Syntax

probe count *times*

undo probe count

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter test type view

Default level

2: System level

Parameters

times: Specifies the number of probe operations per test, in the range of 1 to 15.

Description

Use **probe count** to configure the number of probe operations to be performed per test.

Use **undo probe count** to restore the default.

By default, one probe operation is performed in an NQA test.

In different test types, probe operation has the following different meanings:

- During a TCP or DLSw test, one probe operation means setting up one connection.
- During a UDP jitter or a voice test, one probe operation means continuously sending a specific number of probe packets. The number of probe packets is configurable with the **probe packet-number** command.
- During an FTP, HTTP, DHCP, or DNS test, one probe operation means uploading or downloading a file, obtaining a web page, obtaining an IP address through DHCP, or translating a domain name to an IP address.
- During an ICMP echo or UDP echo test, one probe operation means sending an ICMP echo request or a UDP packet.
- During an SNMP test, one probe operation means sending one SNMPv1 packet, one SNMPv2C packet, and one SNMPv3 packet.

If more than one probe operation is to be performed in a test, the system starts a second probe operation when it receives responses to packets sent in the first probe operation, or when the probe timeout time expires.

This command is not supported by voice tests. Only one probe operation is performed per voice test.

Examples

# Configure the ICMP test group to perform 10 probe operations per test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Syaname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Syntax

probe packet-interval *packet-interval*

undo probe packet-interval

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

packet-interval: Specifies the interval for sending packets per probe operation, in the range of 10 to 60000 milliseconds.

Description

Use **probe packet-interval** to configure the interval for sending packets per probe operation.

Use **undo probe-interval** to restore the default.

By default, the interval is 20 milliseconds.

Examples

# Configure the UDP jitter test group to send packets at an interval of 100 milliseconds during each probe operation.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

packet-number: Specifies the number of packets to be sent per probe operation. The value is in the range of 10 to 1000 for each probe operation in one UDP jitter test, and 10 to 60000 for each probe operation in one voice test.

Description

Use **probe packet-number** to configure the number of packets to be sent per probe during one UDP jitter or voice test.

Use **undo probe packet-number** to restore the default.

By default, the number of packets to be sent per probe is 10 in one UDP jitter test and 1000 in one voice test.

Examples

# Configure the UDP jitter test group to send 100 packets per probe.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Syntax

probe packet-timeout *packet-timeout*

undo probe packet-timeout

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

packet-timeout: Specifies the timeout time in milliseconds for waiting for responses in a UDP jitter or voice test. The value is in the range of 10 to 3600000.

Description

Use **probe packet-timeout** to configure the timeout time for waiting for a response in a UDP jitter or voice test.

Use **undo probe packet-timeout** to restore the default.

By default, the timeout time in a UDP jitter test is 3000 milliseconds, the timeout time in a voice test is 5000 milliseconds.

Examples

# Configure the timeout time for waiting for a response in a UDP jitter test as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default level

2: System level

Parameters

timeout: Specifies the timeout time in milliseconds for a probe operation. The value is in the range of 10 to 86400000 for an FTP or HTTP probe operation, and 10 to 3600000 for a DHCP, DNS, DLSw, ICMP echo, SNMP, TCP, or UDP echo probe operation.

Description

Use **probe timeout** to configure the timeout time for a probe operation. When a probe operation does not complete within the period, the probe operation is timed out.

Use **undo probe timeout** to restore the default.

By default, the timeout time is 3000 milliseconds for a probe operation.

This command is not supported by UDP jitter or voice tests.

Examples

# Configure the timeout time for a DHCP probe operation as 10000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Syaname-nqa-admin-test-dhcp] probe timeout 10000
```

reaction checked-element icpif

Syntax

reaction *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

Voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-value: Specifies threshold values.

upper-threshold: Specifies an upper threshold, in the range of 1 to 100.

lower-threshold: Specifies a lower threshold, in the range of 1 to 100. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element icpif** to configure a reaction entry for monitoring the ICPIF value in a voice test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring ICPIF values is configured.

Examples

# Create reaction entry 1 for monitoring the ICPIF value in each voice test. Set the upper threshold to 50 and lower threshold to 5. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the ICPIF value is checked. If it is out of the threshold range, the state of the reaction entry is set to over-threshold; otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element icpif threshold-value 50 5
action-type trap-only
```

reaction checked-element { jitter-ds | jitter-sd }

Syntax

reaction *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

jitter-ds: Specifies destination-to-source delay jitter of each probe packet as the monitored element.

jitter-sd: Specifies source-to-destination delay jitter of each probe packet as the monitored element.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 14999 for UDP jitter tests, and 1 to 59999 for voice tests.

average: Specifies to check the average one-way delay jitter in each test.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element** { **jitter-ds** | **jitter-sd** } to configure a reaction entry for monitoring one-way delay jitter in each test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring one-way delay jitter is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

Examples

# Create reaction entry 1 for monitoring the average destination-to-source delay jitter of UDP jitter probe packets. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average destination-to-source delay jitter is checked. If it is out of the threshold range, the state of the reaction

entry is set to over-threshold; otherwise, the state is set to below-threshold. Once state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element jitter-ds threshold-type
average threshold-value 50 5 action-type trap-only
```

# Create reaction entry 2 for monitoring the destination-to-source delay jitter of UDP jitter probe packets. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the destination-to-source delay jitter is checked against the threshold range. If the total number of threshold violations exceeds 100 (included), the state of the entry is set to over-threshold; otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 2 checked-element jitter-ds threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction checked-element mos

Syntax

reaction *item-number* **checked-element** **mos** **threshold-value** *upper-threshold* *lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

Voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-value: Specifies threshold values.

upper-threshold: Specifies an upper threshold, in the range of 1 to 500.

lower-threshold: Specifies a lower threshold, in the range of 1 to 500. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element mos** to configure a reaction entry for monitoring the MOS value in each voice test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the MOS value is configured.

For the MOS threshold, the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 1, enter 100.

Examples

# Create reaction entry 1 for monitoring the MOS value of each voice test. Set the upper threshold to 2, and lower threshold to 1. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the MOS value is checked. If it is out of the threshold range, the state of the reaction entry is set to over-threshold; otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element mos threshold-value 200 100
action-type trap-only
```

reaction checked-element { owd-ds | owd-sd }

Syntax

reaction *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold*

undo reaction *item-number*

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

owd-ds: Specifies the destination-to-source delay of each probe packet as the monitored element.

owd-sd: Specifies the source-to-destination delay of each probe packet as the monitored element.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

Description

Use **reaction checked-element** { **owd-ds** | **owd-sd** } to configure a reaction entry for monitoring the one-way delay. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the one-way delay is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

No actions can be configured for a reaction entry of monitoring one-way delays. The monitoring results and statistics, however, can be displayed by the **display nqa reaction counters** and **display nqa statistics** commands.

Examples

# Create reaction entry 1 for monitoring the destination-to-source delay of every UDP jitter probe packet. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. The destination-to-source delay is calculated after the response to the probe packet arrives. If the delay is out of the threshold range, the state of the reaction entry is set to over-threshold; otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element owd-ds threshold-value 50
5
```

reaction checked-element packet-loss

Syntax

reaction *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of lost packets in a test. The value is in the range of 1 to 15000 for UDP jitter tests and 1 to 60000 for voice tests.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element packet-loss** to configure a reaction entry for monitoring the packet loss in each test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the packet loss is configured.

Examples

# Create reaction entry 1 for monitoring the packet loss in each UDP jitter test. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the packet loss is checked. If the total number of lost packets exceeds 100 (included), the state of the reaction entry is set to over-threshold; otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element packet-loss
threshold-type accumulate 100 action-type trap-only
```

reaction checked-element probe-duration

Syntax

reaction *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

DHCP, DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 15.

average: Specifies to check the average probe duration in each test.

consecutive *consecutive-occurrences*: Specifies the number of consecutive threshold violations since the NQA test group starts. The value is in the range of 1 to 16.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages. This keyword is not supported in DNS test view.

Description

Use **reaction checked-element probe-duration** to configure a reaction entry for monitoring the probe duration. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the probe duration is configured.

Only successful probes are monitored. The duration of a failed probe is not counted.

Examples

# Create reaction entry 1 for monitoring the average duration of ICMP echo probes in a test. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average probe duration is checked. If it is out of the threshold range, the state is set to over-threshold; otherwise, the state of the reaction entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-duration
threshold-type average threshold-value 50 5 action-type trap-only
```

# Create reaction entry 2 for monitoring the duration of ICMP echo probes in a test. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the probe duration is checked against the threshold range. If the total number of threshold violations exceeds 10 (included), the state of the entry is set to over-threshold; otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-duration
threshold-type accumulate 10 threshold-value 50 5 action-type trap-only
```

# Create reaction entry 3 for monitoring the duration time of ICMP echo probes. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. The probe duration is checked against the threshold range for each probe. If a threshold violation occurs consecutively for 10 times or more since the test group starts, the state of the entry is set to over-threshold; otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 3 checked-element probe-duration
threshold-type consecutive 10 threshold-value 50 5 action-type trap-only
```

reaction checked-element probe-fail (for trap)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

DHCP, DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of probe failures in a test. The value is in the range of 1 to 15.

consecutive *consecutive-occurrences*: Specifies the number of consecutive probe failures since the NQA test group starts. The value is in the range of 1 to 16.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages. This keyword is not supported in DNS test view.

Description

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe failures. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring probe failures is configured.

Examples

# Create reaction entry 1 for monitoring the probe failures in ICMP echo tests. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, if the total number of probe failures exceeds 10 (included), the state of the entry is set to over-threshold; otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
accumulate 10 action-type trap-only
```

# Create reaction entry 2 for monitoring the probe failures in ICMP echo tests. Before the NQA test group starts, the initial state of the reaction entry is invalid. If probe failure occurs consecutively for 10 times or more since the test group starts, the state of the entry is set to over-threshold; otherwise, the state of the

entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type
consecutive 10 action-type trap-only
```

reaction checked-element probe-fail (for trigger)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

consecutive *consecutive-occurrences*: Specifies the number of consecutive probe failures since the test group starts. The value is in the range of 1 to 16.

action-type: Specifies what actions to be triggered to react to certain measurement conditions.

trigger-only: Triggers other modules to react to certain conditions.

Description

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe results of the current test group. If the number of consecutive probe failures reaches the threshold, collaboration with other modules is triggered. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to remove the specified reaction entry.

By default, no reaction entries are configured.

The collaboration function is not supported by UDP jitter or voice tests.

Related commands: **track** (High Availability Command Reference).

Examples

# Create reaction entry 1. If probe failure occurs consecutively for 3 times, collaboration with other modules is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

reaction checked-element rtt

Syntax

reaction *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

UDP jitter, voice test type view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 15000 for UDP jitter tests and 1 to 60000 for voice tests.

average: Specifies to check the packet average round-trip time in a test.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element rtt** to configure a reaction entry for monitoring packet round-trip time. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring packet round-trip time is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

Examples

# Create reaction entry 1 for monitoring the average round-trip time of UDP jitter probe packets. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average packet round-trip time is checked. If it is out of the threshold range, the state is set to over-threshold; otherwise, the state is set to below-threshold. Once the reaction entry state changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
```

```
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
average threshold-value 50 5 action-type trap-only
```

# Create reaction entry 2 for monitoring the round-trip time of UDP jitter probe packets. Set the upper threshold to 50 milliseconds, and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the packet round-trip time is checked against the threshold range. If the total number of threshold violations exceeds 100 (included), the state of the entry is set to over-threshold; otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction trap

Syntax

reaction trap { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** *cumulate-probe-failures* }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

View

Any NQA test type view

Default level

2: System level

Parameters

probe-failure *consecutive-probe-failures*: Sends a trap to the network management server if the number of consecutive probe failures in one test is greater than or equal to *consecutive-probe-failures*. The value for *consecutive-probe-failures* is in the range of 1 to 15. During the test, the system counts the number of consecutive probe failures after each probe operation, so multiple traps might be sent.

test-complete: Sends a trap to indicate that the test is completed.

test-failure *cumulate-probe-failures*: Sends a trap if the total probe failures in an test is greater than or equal to *cumulate-probe-failures*. The value for *cumulate-probe-failures* is in the range of 1 to 15. The system counts the total probe failures after the test completes, so one trap at most is sent.

Description

Use **reaction trap** to configure the sending of traps to the network management server under specified conditions.

Use **undo reaction trap** to restore the default.

By default, no traps are sent to the network management server.

Only the **reaction trap test-complete** command is supported by voice tests.

Examples

# Configure the system to send a trap if consecutive probe failures in an ICMP echo test is greater than or equal to 5.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

View

DNS test type view

Default level

2: System level

Parameters

domain-name: Specifies the domain name to be resolved. It is a case-insensitive string separated by dots (.), each part consisting of 1 to 63 characters. The total length must be within 255 characters, Valid characters in a part include letters, digits, hyphens (-), and underscores (_).

Description

Use **resolve-target** to set the domain name for a DNS test.

Use **undo resolve-target** to restore the default.

By default, no domain name is configured.

Examples

# Set the domain name for DNS resolution to **domain1**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dns
[Syaname-nqa-admin-test-dns] resolve-target domain1
```

route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

None

Description

Use **route-option bypass-route** to enable the routing table bypass function to test the direct connectivity to the direct destination.

Use **undo route-option bypass-route** to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

When the routing table bypass function is enabled, the routing table is not searched, and the packet is sent directly to the destination in a directly connected network.

Examples

# Enable the routing table bypass function.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface

Syntax

source interface *interface-type interface-number*

undo source interface

View

ICMP echo test type view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **source interface** to configure the source interface for ICMP echo request packets. The ICMP echo request packets take the IP address of the source interface as their source IP address. The specified source interface must be up; otherwise, no ICMP echo requests can be sent out.

Use **undo source interface** to restore the default.

By default, no source interface is configured for ICMP echo request packets.

If you configure both the **source interface** command and the **source ip** command, the **source ip** command takes effect.

Related commands: **source ip**.

Examples

# Specify the IP address of interface VLAN-interface 2 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface vlan-interface 2
```

source ip

Syntax

source ip *ip-address*

undo source ip

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

ip-address: Specifies the source IP address of a test operation.

Description

Use **source ip** to configure the source IP address of probe packets. The specified source IP address must be the IP address of a local interface. The local interface must be up; otherwise, no probe packets can be sent out.

Use **undo source ip** to remove the configured source address. The IP address of the interface that sends a probe packet serves as the source IP address of the probe packet.

By default, no source IP address is configured for probe packets.

If you configure both the **source interface** command and the **source ip** command, the **source ip** command takes effect.

Related commands: **source interface**.

Examples

# Configure the source IP address of the ICMP echo packets as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

source port

Syntax

source port *port-number*

undo source port

View

SNMP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

port-number: Specifies the source port number of probe packets, in the range of 1 to 50000.

Description

Use **source port** to configure the source port of probe packets.

Use **undo source port** to remove the configured port number.

By default, no source port number is configured.

Examples

# Configure port 8000 as the source port of probe packets in the UDP echo test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

hold-time: Specifies the hold time of a statistics group in minutes, in the range of 1 to 1440.

Description

Use **statistics hold-time** to configure the hold time of statistics groups for a test group. A statistics group is deleted when its hold time expires.

Use **undo statistics hold-time** to restore the default.

By default, the hold time of a statistics group is 120 minutes.

This command is not supported by DHCP tests.

Examples

# Configure the hold time of a statistics group as 3 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

number: Specifies the maximum number of statistics groups that can be kept, in the range of 0 to 100. To disable collecting statistics, specify number 0.

Description

Use **statistics max-group** to configure the maximum number of statistics groups that can be kept.

Use **undo statistics max-group** to restore the default.

By default, 2 statistics groups at most can be kept.

When the number of statistics groups kept reaches the upper limit and a new statistics group is to be saved, the earliest statistics group is deleted.

This command is not supported by DHCP tests.

Examples

# Configure the NQA to save up to 5 statistics groups for the ICMP test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

statistics interval

Syntax

statistics interval *interval*

undo statistics interval

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

interval: Specifies the interval in minutes for collecting statistics of the test results for a test group, in the range of 1 to 35791394.

Description

Use **statistics interval** to configure the interval for collecting test result statistics for a test group.

Use **undo statistics interval** to restore the default.

By default, the interval is 60 minutes.

NQA groups tests completed in the specified interval, and calculates the test result statistics. The statistics form a statistics group. To view information about the statistics groups, use the **display nqa statistics** command.

This command is not supported by DHCP tests.

Examples

# Configure the interval for collecting the test result statistics of an ICMP test group as 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

tos

Syntax

tos *value*

undo tos

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice, DHCP test type view

Default level

2: System level

Parameters

value: Specifies the value of the ToS (Type of Service) field in the IP header in an NQA probe packet, in the range of 0 to 255.

Description

Use **tos** to configure the value of the ToS field in the IP header in an NQA probe packet.

Use **undo tos** to restore the default.

By default, the ToS field in the IP header of an NQA probe packet is 0.

Examples

# Configure the ToS field in an IP packet header in an NQA probe packet as 1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

ttl

Syntax

ttl *value*

undo ttl

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default level

2: System level

Parameters

value: Specifies the maximum number of hops that a probe packet traverses in the network, in the range of 1 to 255.

Description

Use **ttl** to configure the maximum number of hops that a probe packet traverses in the network.

Use **undo ttl** to restore the default.

By default, the maximum number of hops that a probe packet can traverse in a network is 20.

After you configure the **route-option bypass-route** command, the maximum number of hops that a probe packet traverses in the network is 1, and the **ttl** command does not take effect.

Examples

# Configure the maximum number of hops that a probe packet can traverse in a network as 16.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

type

Syntax

type { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }

View

NQA test group view

Default level

2: System level

Parameters

dhcp: Specifies a DHCP test.

dlsw: Specifies a DLSw test.

dns: Specifies a DNS test.

ftp: Specifies an FTP test.

http: Specifies an HTTP test.

icmp-echo: Specifies an ICMP echo test.

snmp: Specifies an SNMP test.

tcp: Specifies a TCP test.

udp-echo: Specifies a UDP echo test.

udp-jitter: Specifies a UDP jitter test.

voice: Specifies a voice test.

Description

Use **type** to configure the test type of the current test group and enter test type view.

By default, no test type is configured.

Examples

# Configure the test type of a test group as **FTP** and enter test type view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Syntax

url *url*

undo url

View

HTTP test type view

Default level

2: System level

Parameters

url: Specifies the website that an HTTP test visits, a case-sensitive string of 1 to 185 characters.

Description

Use **url** to configure the website that an HTTP test visits.

Use **undo url** to remove the configured website that an HTTP test visits.

The character string of the configured URL cannot contain spaces.

Examples

# Configure the website that an HTTP test visits as /index.htm.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url /index.htm
```

username (FTP test type view)

Syntax

username *username*

undo username

View

FTP test type view

Default level

2: System level

Parameters

username: Specifies the username that is used to log in to the FTP server. The username takes a case-sensitive string of 1 to 32 characters.

Description

Use **username** to configure a username used to log onto the FTP server.

Use **undo username** to remove the configured username.

By default, no username is configured for logging onto the FTP server.

Related commands: **password** and **operation**.

Examples

# Configure the login username as **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

NQA server configuration commands

IMPORTANT:

You only need to configure the NQA server for UDP jitter, TCP, UDP echo and voice tests.

display nqa server status

Syntax

display nqa server status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display nqa server status** to display NQA server status.

Examples

# Display NQA server status.

```
<Sysname> display nqa server status
nqa server is: enabled
tcp-connect:
    IP Address      Port           Status
    2.2.2.2        2000           active
udp-echo:
    IP Address     Port            Status
    3.3.3.3        3000            inactive
```

Table 38 Command output

Field	Description
tcp-connect	NQA server status in the NQA TCP test.
udp-echo	NQA server status in the NQA UDP test.
IP Address	IP address specified for the TCP/UDP listening service on the NQA server.
Port	Port number of the TCP/UDP listening service on the NQA server.
Status	Listening service status, which can be one of the following values: • **active**—Listening service is ready. • **inactive**—Listening service is not ready.

nqa server enable

Syntax

nqa server enable

undo nqa server enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **nqa server enable** to enable the NQA server.

Use **undo nqa server enable** to disable the NQA server.

By default, the NQA server is disabled.

Related commands: **nqa server tcp-connect**, **nqa server udp-echo**, and **display nqa server status**.

Examples

# Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa server enable
```

nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number*

undo nqa server tcp-connect *ip-address port-number*

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address specified for the TCP listening service on the NQA server.

port-number: Specifies the port number specified for the TCP listening service on the NQA server, in the range of 1 to 50000.

Description

Use **nqa server tcp-connect** to create a TCP listening service on the NQA server.

Use **undo nqa server tcp-connect** to remove the TCP listening service created.

Configure the command on the NQA server for TCP tests only.

The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.

The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

# Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

nqa server tcp-connect tos

Syntax

nqa server tcp-connect tos *tos*

undo nqa server tcp-connect tos

View

System view

Default level

2: System level

Parameters

tos: Specifies the value of the ToS field, in the range of 0 to 255.

Description

Use **nqa server tcp-connect tos** to configure the ToS value in the packets sent by TCP listening service on the NQA server.

Use **undo nqa server tcp-connect tos** to restore the default value.

By default, the ToS value is 0.

Examples

# Set the ToS value to 30 in the packets sent by the TCP listening service on the NQA server,

```
<Sysname> system-view
[Sysname] nqa server tcp-connect tos 30
```

nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number*

undo nqa server udp-echo *ip-address port-number*

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address specified for the UDP listening service on the NQA server.

port-number: Specifies the port number specified for the UDP listening service on the NQA server, in the range of 1 to 50000.

Description

Use **nqa server udp-echo** to create a UDP listening service on the NQA server.

Use **undo nqa server udp-echo** to remove the UDP listening service created.

Configure the command on the NQA server for UDP jitter, UDP echo and voice tests only.

The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service.

The IP address must be that of an interface on the NQA server. Otherwise, the configuration becomes invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

# Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

nqa server udp-echo tos

Syntax

nqa server udp-echo tos *tos*

undo nqa server udp-echo tos

View

System level

Default level

2: System level

Parameters

tos: Specifies the value of the ToS field, in the range of 0 to 255.

Description

Use **nqa server udp-echo tos** to configure the ToS value in the packets sent by the UDP listening service on the NQA server.

Use **undo nqa server udp-echo tos** to restore the default value.

By default, the ToS value is 0.

Examples

# Set the ToS value to 30 in the packets sent by the UDP listening service enabled on the NQA server.

```
<Sysname> system-view
[Sysname] nqa server udp-echo tos 30
```

sFlow configuration commands

display sflow

Syntax

display sflow [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Displays the sFlow configuration and operation information of an IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display sflow** to display the sFlow configuration and operation information.

Examples

# Display the sFlow configuration and operation information.

```
<Sysname> display sflow
sFlow Version: 5
sFlow Global Information:
Agent        IP:10.10.10.1 (Auto)
Source  Address:10.0.0.1 2001::1
Collector Information
ID    IP                                   Port  Aging     Size   Description
1     22:2:20::10                          6535   N/A      3000    netserver
2     192.168.3.5                          6543   500      3000    Office
3                                          6343   0        1400
4                                          6343   0        1400
5                                          6343   0        1400
6                                          6343   0        1400
7                                          6343   0        1400
8                                          6343   0        1400
9                                          6343   0        1400
10                                         6343   0        1400
```

```
sFlow Port Information:
Interface CID    Interval(s)  FID MaxHLen   Rate       Mode     Status
GE1/0/1     1     100          1   128       1000       Random   Active
GE1/0/2     2     100          2   128       1000       Random   Active
```

Table 39 Command output

Field	Description
sFlow Version	Currently, sFlow has the following versions, 5: sFlow version 5.
sFlow Global Information	sFlow global configuration information.
Agent	IP address of the sFlow agent: • **CLI**—Manually configured IP address. • **Auto**—Automatically obtained IP address.
Source Address	Source IP address of sent sFlow packets.
Collector Information	sFlow collector information.
ID	sFlow collector ID.
IP	IP address of the sFlow collector that receives sFlow packets.
Port	Number of the port receiving sFlow packets on the sFlow collector.
Aging	The rest time for the sFlow collector to survive. If N/A is displayed, the sFlow collector is never aged out.
Size	The maximum length of the sFlow data portion in every sFlow packet that is sent out.
Description	Description of the sFlow collector.
sFlow Port Information	Information of the ports enabled with sFlow.
Interface	sFlow enabled interface.
CID	ID of the target collector, for receiving the counter sampling data.
Interval(s)	Counter sampling interval, in seconds.
FID	ID of the target collector, for receiving the flow sampling data.
MaxHLen	Maximum copied length of a sampled packet.
Rate	Packet sampling interval.
Mode	Packet sampling mode, which can only be random and samples a random number of packets.
Status	Status of the sFlow enabled port: • **Suspend**—Indicates the port is down. • **Active**—Indicates the port is up.

sflow agent

Syntax

sflow agent { **ip** *ip-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

View

System view

Default level

2: System level

Parameters

ip *ip-address*: Specifies the IPv4 address of the sFlow agent.

ipv6 *ipv6-address*: Specifies the IPv6 address of the sFlow agent.

Description

Use **sflow agent** to configure the IP address of the sFlow agent.

Use **undo sflow agent** to remove the configured IP address.

By default, no IP address is configured for the sFlow agent. The device periodically checks the existence of sFlow agent address. If the sFlow agent has no IP address configured, the device automatically selects an interface IP address for the sFlow agent but does not save the selected IP address.

NOTE:

- HP recommends that you configure an IP address manually for the sFlow agent.
- Only one IP address can be specified for the sFlow agent on the switch.

Examples

# Configure the IP address of the sFlow agent.

```
<Sysname> system-view
[Sysname] sflow agent ip 10.10.10.1
```

sflow collector

Syntax

sflow collector *collector-id* { { **ip** *ip-address* | **ipv6** *ipv6-address* } | **datagram-size** *size* | **description** *text* | **port** *port-number* | **time-out** *seconds* } *

undo sflow collector *collector-id*

View

System view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector. The switch can support ten sFlow collectors.

ip *ip-address*: Specifies the IPv4 address of the sFlow collector.

ipv6 *ipv6-address*: Specifies the IPv6 address of the sFlow collector.

description *text*: Specifies a description for the sFlow collector. The default description is "CLI Collector."

datagram-size *size*: Specifies the maximum length of the sFlow data portion in every sFlow packet that is sent out. The value ranges from 200 to 3000 bytes and defaults to 1400 bytes.

port *port-number*: Specifies the port number of the sFlow collector, in the range of 1 to 65535. The default port number is 6343.

time-out *seconds*: Specifies the aging time of the sFlow collector, in the range of 60 to 2147483647, in seconds. By default, the sFlow collector never ages out. When the aging time expires, all the settings of the sFlow collector are restored to the default. The system does not save the configuration of collectors with an aging time specified.

Description

Use **sflow collector** to configure an sFlow collector.

Use **undo sflow collector** to remove a specified sFlow collector.

By default, the device provides a number of sFlow collectors. You can use the **display sflow** command to display these sFlow collectors.

Examples

# Specify sFlow collector 2's destination IP address as 3.3.3.1, port number as default, description as **netserver**, aging time as 1200 seconds, and maximum length of the sFlow data portion as 1000 bytes.

```
<Sysname> system-view
[Sysname] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size
1000
```

sflow counter interval

Syntax

sflow counter interval *interval-time*

undo sflow counter interval

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

interval-time: Specifies the counter sampling interval in seconds, in the range of 2 to 86400.

Description

Use **sflow counter interval** to set the counter sampling interval.

Use **undo sflow counter interval** to disable sFlow counter sampling.

By default, counter sampling is disabled.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

# Set the counter sampling interval to 120 seconds on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] sflow counter interval 120
```

sflow counter collector

Syntax

sflow counter collector *collector-id*

undo sflow counter collector

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector.

Description

Use **sflow counter collector** to specify the sFlow collector for counter sampling.

Use **undo sflow counter collector** to remove the sFlow collector for counter sampling.

By default, no sFlow collector is specified for counter sampling.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

# Specify sFlow collector 2 on gigabitethernet 1/0/1 for counter sampling.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow counter collector 2
```

sflow flow collector

Syntax

sflow flow collector *collector-id*

undo sflow flow collector

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector.

Description

Use **sflow flow collector** to specify the sFlow collector for flow sampling.

Use **undo sflow flow collector** to remove the sFlow collector configured for flow sampling.

By default, no sFlow collector is specified for flow sampling.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

# Specify the collector number 2 on GigabitEthernet1/0/1 for flow sampling.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] sflow flow collector 2
```

sflow flow max-header

Syntax

sflow flow max-header *length*

undo sflow flow max-header

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

Length: Specifies the maximum bytes of a sampled packet that can be copied, in the range of 18 to 512.

Description

Use **sflow flow max-header** to set the maximum bytes of a sampled packet that can be copied (starting from the header).

Use **undo sflow flow max-header** to restore the default.

By default, up to 128 bytes of a sampled packet that can be copied. HP recommends you use the default value.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces)

# Set the maximum bytes of a sampled packet that can be copied to 60.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow flow max-header 60
```

sflow sampling-mode

Syntax

sflow sampling-mode { **determine** | **random** }

undo sflow sampling-mode

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

determine: Specifies the fixed sampling mode. For example, if the flow sampling interval is set to 4000 (by using the **sflow sampling-rate** command), the device randomly samples a packet, like the tenth packet, from the first 4000 packets. The next time the device samples the 4010th packet, and so on.

random: Specifies the random sampling mode. After the sampling interval is specified with the **sflow sampling-rate** command, a device samples zero, one, or multiple packets from each group of sampled packets. Generally, one packet is sampled from each group of sampled packets. For example, with the packet sampling rate set to 4000, the device may sample one packet from the first 4000 packets, two from the next 4000 packets, and none from the third 4000 packets, but generally the device samples one packet from 4000 packets.

Description

Use **sflow sampling-mode** to specify the packet sampling mode.

Use **undo sflow sampling-mode** to restore the default.

The default mode is **random**.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Related commands: **sflow sampling-rate**.

NOTE:

The switch does not support the flow sampling mode **determine**.

Examples

# Specify the random sample mode on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow sampling-mode random
```

sflow sampling-rate

Syntax

sflow sampling-rate *interval*

undo sflow sampling-rate

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

interval: Specifies the number of packets out of which the interface will sample a packet, ranging from 1000 to 500000.

Description

Use **sflow sampling-rate** to specify the number of packets out of which the interface will sample a packet.

Use **undo sflow sampling-rate** to disable sampling.

By default, packet sampling is disabled.

This command is supported only on Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

The bigger the value of the *interval* argument, the lower the sampling rate, and vice versa.

Related commands: **sflow sampling-mode**.

Examples

# Set GigabitEthernet 1/0/1 to sample a packet out of 4000 packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] sflow sampling-rate 4000
```

sflow source

Syntax

sflow source { **ip** *ip-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

View

System view

Default level

2: System level

Parameters

ip *ip-address*: Specifies the source IPv4 address of sent sFlow packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address of sent sFlow packets.

Description

Use **sflow source** to specify the source IP address of sent sFlow packets.

Use **undo sflow source** to remove the specified source IP address.

By default, no source IP address is specified for sent sFlow packets.

Examples

# Specify the source IPv4 address of sent sFlow packets as 10.0.0.1.

```
<Sysname> system-view
[Sysname] sflow source ip 10.0.0.1
```

IPC configuration commands

The **display** commands for the IPC feature display only information about active nodes.

display ipc channel

Syntax

display ipc channel { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays channel information for a node. The *node-id* argument takes a node number in the range of 0 to 10.

self-node: Displays channel information for the local node.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc channel** to display channel information for a node.

Examples

# Display channel information for node **1**.

```
<Sysname> display ipc channel node 1
ChannelID      Description
------------------------------------------------
19             RPC channel
72             Portal Backup Channel
79             DHCP
94             IPC test channel
149            Prehistorical channel, NO.1
```

Table 40 Command output

Field	Description
ChannelID	Channel number, which has been predefined and assigned by the system. One channel number corresponds to one module. The **display ipc channel** command displays the numbers of the current active modules.
Description	Description information, which is generated by the internal software of the device, is used to describe the functions of a channel. For example, "FIB4" indicates that the channel is used for Layer 3 fast forwarding; "Prehistorical channel, NO.2" indicates that no description is defined for the channel, and the channel is the second channel established.

display ipc link

Syntax

display ipc link { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the link status of the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the link status of the local node.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc link** to display the link status of the specified node.

Examples

# Display link status information for the local node.

```
<Sysname> display ipc link self-node
Dst-NodeID         LinkStatus
-------------------------------------------
1                   UP
2                   DOWN
```

The output shows that:

- An UP connection exists between the local node and node 1.
- A DOWN connection exists between the local node and node 2.

Table 41 Command output

Field	Description
Dst-NodeID	Number of the peer node.
LinkStatus	Link status: **UP**—A connection is established. **DOWN**—A connection is terminated.

display ipc multicast-group

Syntax

display ipc multicast-group { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the multicast group information for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the multicast group information for the local node.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc multicast-group** to display the multicast group information for the specified node.

Examples

# Display the multicast group information for node **1**.

```
<Sysname> display ipc multicast-group node 1
GroupID    Status    ChannelID
----------------------------------
8           INUSE      12
```

Table 42 Command output

Field	Description
GroupID	Multicast group ID.

Field	Description
Status	Link status: **INUSE**—The multicast group is in use. **DELETE**—The multicast group is to be deleted.
ChannelID	Channel number.

display ipc node

Syntax

display ipc node [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc node** to display node information.

Examples

# Display node information for the device.

```
<Sysname> display ipc node
Self node ID: 1
Current active node ID: 1
```

Table 43 Command output

Field	Description
Self node ID	Number of the local node
Current active node ID	List of the current active nodes

display ipc packet

Syntax

display ipc packet { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the packet statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the packet statistics for the local node.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc packet** to display the packet statistics for the specified node.

Examples

# Display the packet statistics for the local node.

```
<Sysname> display ipc packet self-node
ChannelID Sent-fragments Sent-packets Received-fragments Received-packets
--------------------------------------------------------------------------
11          828              810            819                   810
13          0                0               0                     0
14          5                3               5                     5
15          0                0               0                     0
16          0                0               0                     0
17          50               50             37                    35
19          0                0               0                     0
```

Table 44 Command output

Field	Description
ChannelID	Channel number.
Sent-fragments	Number of fragments sent.
Sent-packets	Number of packets sent. Whether a packet is fragmented depends on the interface MTU and the packet size in bytes. If the packet size is larger than the MTU, the packet is fragmented. If the packet size is smaller than or equal to the MTU, the packet is sent.
Received-fragments	Number of fragments successfully received.
Received-packets	Number of packets successfully received. If fragments are received on an interface, the system reassembles the fragments and sends a complete packet to the upper layer.

display ipc performance

Syntax

display ipc performance { **node** *node-id* | **self-node** } [**channel** *channel-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the IPC performance statistics for the local node.

channel *channel-id*: Displays the IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc performance** to display IPC performance statistics.

If IPC performance statistics is enabled, the command displays the current IPC performance statistics. If IPC performance statistics is disabled, the command displays the IPC performance statistics collected before IPC performance statistics was disabled.

Related commands: **ipc performance enable**.

Examples

# Display the IPC performance statistics for node **1**.

```
<Sysname> display ipc performance node 1
Peak: Peak rate (pps)
10Sec: Average rate in the last 10 seconds (pps)
1Min: Average rate in the last 1  minute (pps)
5Min: Average rate in the last 5  minutes (pps)
Total-Data: Total number of data (packets)

Statistics for packets sent successfully:
Peak        10Sec         1Min        5Min        Total-Data
------------------------------------------------------------
1             1              1            0            80
```

```
Statistics for packets recieved successfully:
Peak        10Sec          1Min        5Min        Total-Data
------------------------------------------------------------
1            1              1           0            82
Statistics for packets acknowledged:
Peak        10Sec          1Min        5Min        Total-Data
------------------------------------------------------------
1            1              1           0            78
```

Table 45 Command output

Field	Description
Peak	Peak rate in pps (average rate is measured every 10 seconds, the greatest value of which is taken as the peak rate).
10Sec	Average rate (in pps) for the past 10 seconds.
1Min	Average rate (in pps) for the past 1 minute.
5Min	Average rate (in pps) for the past 5 minutes.
Total-Data	Total amount of data collected from the time when IPC performance statistics was enabled to the time when this command was executed.

display ipc queue

Syntax

display ipc queue { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the sending queue information for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the sending queue information for the local node.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipc queue** to display the sending queue information for the specified node.

Examples

# Display the sending queue information for the local node.

```
<Sysname> display ipc queue self-node
QueueType  QueueID Dst-NodeID   Length  FullTimes   Packet
------------------------------------------------------------
UNICAST      0         0             4096     0             0
UNICAST      1         0             4096     0             0
UNICAST      2         0             4096     0             0
UNICAST      3         0             4096     0             0
UNICAST      0         1             4096     0             0
UNICAST      1         1             4096     0             0
UNICAST      2         1             4096     0             0
UNICAST      3         1             4096     0             0
MULTICAST    0         --            4096     0             0
MULTICAST    1         --            4096     0             0
MULTICAST    2         --            512      0             0
MULTICAST    3         --            512      0             0
MULTICAST    4         --            512      0             0
MULTICAST    5         --            512      0             0
MIXCAST      0         --            2048     0             0
MIXCAST      1         --            2048     0             0
```

Table 46 Command output

Field	Description
QueueType	Queue type: • **UNICAST**—Unicast queue. • **MULTICAST**—Multicast (including broadcast) queue. • **MIXCAST**—Mixcast queue, which can accommodate unicasts, multicasts, and broadcasts.
QueueID	Queue number.
Dst-NodeID	Peer node number. If no peer node exists, two hyphens (--) are displayed.
Length	Queue length (number of packets that can be buffered).
FullTimes	Number of times the queue was full.
Packet	Total number of packets in the queue.

ipc performance enable

Syntax

ipc performance enable { **node** *node-id* | **self-node** } [**channel** *channel-id*]

undo ipc performance enable [**node** *node-id* | **self-node**] [**channel** *channel-id*]

View

User view

Default level

1: Monitor level

Parameters

node *node-id*: Enables IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Enables IPC performance statistics for the local node.

channel *channel-id*: Enables IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

Description

Use **ipc performance enable** to enable IPC performance statistics. Use the **undo ipc performance** command to disable IPC performance statistics.

By default, IPC performance statistics is disabled.

When IPC performance statistics is disabled, the statistics data does not change. The **display ipc performance** command displays the statistics collected before IPC performance statistics was disabled.

Examples

# Enable IPC performance statistics of channel **18** on node **1**.

```
<Sysname> ipc performance enable node 1 channel 18
```

reset ipc performance

Syntax

reset ipc performance [**node** *node-id* | **self-node**] [**channel** *channel-id*]

View

User view

Default level

1: Monitor level

Parameters

node *node-id*: Clears the IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Clears the IPC performance statistics for the local node.

channel *channel-id*: Clears the IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

Description

Use **reset ipc performance** to clear IPC performance statistics.

Examples

# Clear the IPC performance statistics of channel 18 on node 1.

```
<Sysname> reset ipc performance node 1 channel 18
```

PoE configuration commands

apply poe-profile

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

View

PoE interface view

Default level

2: System level

Parameters

index *index*: Specifies the index number of the PoE configuration file, in the range of 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file, a string of 1 to 15 characters.

Description

Use **apply poe-profile** to apply the PoE configuration file to the current PoE interface.

Use **undo apply poe-profile** to remove the application of the PoE configuration file to the current PoE interface.

The index number, instead of the name, of the PoE configuration file is displayed when you execute the **display this** command.

Related commands: **display poe-profile** and **apply poe-profile interface**.

Examples

# Apply the PoE configuration file named **forIPphone** to PoE interface GigabitEthernet 1/0/20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/20
[Sysname-GigabitEthernet1/0/20] apply poe-profile name forIPphone
[Sysname-GigabitEthernet1/0/20] display this
#
interface GigabitEthernet1/0/20
 apply poe-profile index 1
#
return
```

apply poe-profile interface

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

View

System view

Default level

2: System level

Parameters

index *index*: Specifies the index number of the PoE configuration file, in the range of 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file, a string of 1 to 15 characters.

interface-range: Specifies a range of Ethernet interface numbers, indicating multiple Ethernet interfaces. The expression is *interface-range* = *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number should be smaller than the end interface number. Ethernet interface numbers can be in any range. If any interface in the specified range does not support PoE, it is ignored when the PoE configuration file is applied.

Description

Use **apply poe-profile interface** to apply the PoE configuration file to one or more PoE interfaces.

Use **undo apply poe-profile interface** to remove the application of the PoE configuration file to the specified PoE interfaces.

Related commands: **display poe-profile interface** and **apply poe-profile**.

Examples

# Apply the PoE configuration file named **forIPphone** to PoE interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] apply poe-profile name forIPphone interface gigabitethernet 1/0/1
```

# Apply the PoE configuration file with index number 1 to PoE interfaces GigabitEthernet 1/0/2 through GigabitEthernet 1/0/8.

```
<Sysname> system-view
[Sysname] apply poe-profile index 1 interface gigabitethernet 1/0/2 to gigabitethernet
1/0/8
```

display poe device

Syntax

display poe device [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe device** to display information about PSEs.

Examples

# Display PSE information. The output depends on the device model.

```
<Sysname> display poe device
PSE ID  SlotNo SubSNo PortNum  MaxPower(W)  State  Model
 4       1      0      24       370          off    PD67024
```

Table 47 Command output

Field	Description
PSE ID	ID of the PSE.
SlotNo	Slot number of the PSE.
SubSNo	Sub-slot number of the PSE.
PortNum	Number of PoE interfaces on the PSE.
MaxPower(W)	Maximum power of the PSE (W).
State	PSE state: • **on**—The PSE is supplying power. • **off**—The PSE stops supplying power. • **faulty**—The PSE fails.
Model	PSE model.

display poe interface

Syntax

display poe interface [*interface-type interface-number*] [**\|** { **begin** \| **exclude** \| **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe interface** to display the power information of the specified interface.

If no interface is specified, the power information of all PoE interfaces is displayed.

Examples

# Display the power state of GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1
 Port Power Enabled               : enabled
 Port Power Priority              : high
 Port Operating Status            : on
 Port IEEE Class                   : 0
 Port Detection Status            : delivering-power
 Port Power Mode                   : signal
 Port Current Power                : 3600     mW
 Port Average Power                : 3662     mW
 Port Peak Power                   : 3900     mW
 Port Max Power                    : 15400    mW
 Port Current                      : 71       mA
 Port Voltage                      : 50.9     V
 Port PD Description              :  IP Phone For Room 101
```

Table 48 Command output

Field	Description
Port Power Enabled	**PoE state**—Enabled or disabled.
Port Power Priority	Power priority of the PoE interface: - critical (highest) - high - low
Port Operating Status	Operating state of a PoE interface: - **off**—PoE is disabled. - **on**—Power is supplied for a PoE interface normally. - **power-lack**—The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. - **power-deny**—The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. - **power-itself**—The external equipment is supplying power for itself. - **power-limit**—The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
Port IEEE class	PD power class: 0, 1, 2, 3, 4, and a hyphen (-). The hyphen (-) indicates not supported.

Field	Description
Port Detection Status	Power detection state of a PoE interface: • **disabled**—The PoE function is disabled. • **searching**—The PoE interface is searching for the PD. • **delivering-power**—The PoE interface is supplying power for the PD. • **fault**—There is a fault defined in 802.3af. • **test**—The PoE interface is under test. • **other-fault**—There is a fault other than defined in 802.3af. • **pd-disconnect**—The PD is disconnected.
Port Power Mode	Power mode of a PoE interface. **signal** indicates that power is supplied over signal cables.
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss. The transmission loss usually does not exceed one watt.
Port Average Power	Average power of a PoE interface.
Port Peak Power	Peak power of a PoE interface.
Port Max Power	Maximum power of a PoE interface.
Port Current	Current of a PoE interface.
Port Voltage	Voltage of a PoE interface.
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

# Display the state of all PoE interfaces.

```
<Sysname> display poe interface
 Interface  Status   Priority  CurPower  Operating    IEEE   Detection
                                    (W)        Status       Class  Status
 GE1/0/1      enabled  high     3.6      on         0      delivering-power
 GE1/0/2      enabled  low      0.0      off        0      searching
 GE1/0/3      enabled  low      0.0      off        0      searching
 GE1/0/4      enabled  low      0.0      off        0      searching
 GE1/0/5      enabled  low      0.0      off        0      searching
 GE1/0/6      enabled  low      0.0      off        0      searching
 GE1/0/7      enabled  low      0.0      off        0      searching
 GE1/0/8      enabled  low      0.0      off        0      searching
 ……
 GE1/0/23      enabled  low      0.0      off        0      searching
 GE1/0/24      enabled  low      0.0      off        0      searching

  ---  1 port(s) on,   3.6 (W) consumed,   367.4 (W) remaining ---
```

Table 49 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Enable	PoE state—enabled or disabled.

Field	Description
Priority	Power priority of a PoE interface: • critical (highest) • high • low
CurPower	Current power of a PoE interface.
Operating Status	Operating state of a PoE interface: • **off**—PoE is disabled. • **on**—Power is supplied for a PoE interface normally. • **power-lack**—The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. • **power-deny**—The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. • **power-itself**—The external equipment is supplying power for itself. • **power-limit**—The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
IEEE class	PD power class defined by IEEE.
Detection Status	Power detection state of a PoE interface: • **disabled**—The PoE function is disabled. • **searching**—The PoE interface is searching for the PD. • **delivering-power**—The PoE interface is supplying power for the PD. • **fault**—There is a fault defined in 802.3af. • **test**—The PoE interface is under test. • There is a fault other than defined in 802.3af. • **pd-disconnect**—The PD is disconnected.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by the current PoE interface.
Remaining	Remaining power that the PSE can still supply.

display poe interface power

Syntax

display poe interface power [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe interface power** to display the power statistics for PoE interfaces.

If no interface is specified, the power statistics for all PoE interfaces are displayed.

Examples

# Display the power statistics for GigabitEthernet 1/0/1.

```
<Sysname>display poe interface power GigabitEthernet 1/0/1
 Interface    CurPower  PeakPower   MaxPower  PD Description
               (W)        (W)          (W)
 GE1/0/1     0.0        0.0         30.0
```

# Display the power statistics for all PoE interfaces.

```
<Sysname> display poe interface power
 Interface    CurPower  PeakPower   MaxPower  PD Description
               (W)       (W)         (W)
 GE1/0/1     0.0       0.0         30.0
 GE1/0/2     0.0       0.0         30.0
 GE1/0/3     0.0       0.0         30.0
 GE1/0/4     0.0       0.0         30.0
 GE1/0/5     0.0       0.0         30.0
 GE1/0/6     0.0       0.0         30.0
 GE1/0/7     0.0       0.0         30.0
 GE1/0/8     0.0       0.0         30.0
 ……
 GE1/0/23    0.0       0.0         30.0
 GE1/0/24    0.0       0.0         30.0
   --- 0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 50 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power currently consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe pse

Syntax

display poe pse [*pse-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse-id: Specifies the PSE ID. To view the mapping between PSE ID and slot, use the **display poe device** command. If you do not specify this parameter, information about all PSEs is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe pse** to display PSE power information.

Examples

# Display information about the PSE.

```
<Sysname> display poe pse
 PSE ID                            : 4
 PSE Slot No                       : 1
 PSE SubSlot No                    : 0
 PSE Model                         : PD67024
 PSE Power Enabled                 : enabled
 PSE Power Priority                : -
 PSE Current Power                 : 0        W
 PSE Average Power                 : 0        W
 PSE Peak Power                    : 0        W
 PSE Max Power                     : 370      W
 PSE Remaining Guaranteed          : 370      W
 PSE CPLD Version                  : -
 PSE Software Version              : 400
 PSE Hardware Version              : 57603
 PSE Legacy Detection              : disabled
 PSE Utilization-threshold         : 80
 PSE Pd-policy Mode                : disable
 PSE PD Disconnect Detect Mode     : AC
```

Table 51 Command output

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Member of the PSE
PSE SubSlot No	Subslot number of the PSE
PSE Model	Model of the PSE module
PSE Power Enabled	PoE state, enabled or disabled
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE– the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: • Enabled • Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

display poe pse interface

Syntax

display poe pse *pse-id* **interface** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To view the mapping between PSE ID and slot, use the **display poe device** command.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe pse interface** to display the state of all PoE interfaces connected to the specified PSE.

Examples

# Display the power state of all PoE interfaces connected to PSE 4.

```
<Sysname> display poe pse 4 interface
 Interface    Status   Priority CurPower Operating  IEEE   Detection
                                (W)      Status     Class  Status
 GE1/0/1      disabled low      0.0      off        0      disabled
 GE1/0/2      disabled low      0.0      off        0      disabled
 GE1/0/3      disabled low      0.0      off        0      disabled
 GE1/0/4      disabled low      0.0      off        0      disabled
 GE1/0/5      disabled low      0.0      off        0      disabled
 GE1/0/6      disabled low      0.0      off        0      disabled
 GE1/0/7      disabled low      0.0      off        0      disabled
 GE1/0/8      disabled low      0.0      off        0      disabled
 ……
 GE1/0/23     disabled low      0.0      off        0      disabled
 GE1/0/24     disabled low      0.0      off        0      disabled
   ---  0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 52 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Status	PoE enabled/disabled state. For the value, see Table 48.
Priority	Priority of a PoE interface. For the value, see Table 48.
CurPower	Current power of a PoE interface.
Operating Status	Operating state of a PoE interface. For the value, see Table 48.
IEEE Class	PD power class.
Detection Status	Power detection state of a PoE interface. For the value, see Table 48.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by PoE interfaces on the PSE.
Remaining	Remaining power that the PSE can still supply.

display poe pse interface power

Syntax

display poe pse *pse-id* **interface power** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To view the mapping between PSE ID and slot, use the **display poe device** command.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe pse interface power** to display the power information of PoE interfaces connected with the PSE.

Examples

# Display the power state of PoE interfaces connected with PSE 4.

```
<Sysname> display poe pse 4 interface power
 Interface   CurPower  PeakPower   MaxPower   PD Description
              (W)        (W)           (W)
 GE1/0/1     0.0       0.0         30.0
 GE1/0/2     0.0       0.0         30.0
 GE1/0/3     0.0       0.0         30.0
 GE1/0/4     0.0       0.0         30.0
 GE1/0/5     0.0       0.0         30.0
 GE1/0/6     0.0       0.0         30.0
 GE1/0/7     0.0       0.0         30.0
 GE1/0/8     0.0       0.0         30.0
 ......
 GE1/0/23    0.0       0.0         30.0
 GE1/0/24    0.0       0.0         30.0
   ---  0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 53 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.

Field	Description
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power being consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe-profile

Syntax

display poe-profile [**index** *index* | **name** *profile-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

index *index*: Specifies the index number of the PoE configuration file, in the range of 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file, a string of 1 to 15 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe-profile** to display the information of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files is displayed.

Examples

# Display the information of all PoE configuration files.

```
<Sysname> display poe-profile
 Poe-profile     Index   ApplyNum  Interface   Configuration
forIPphone      1        6          GE1/0/5        poe enable
                                       GE1/0/6         poe priority critical
                                       GE1/0/7
                                       GE1/0/8
                                       GE1/0/9
                                       GE1/0/10
 forAP            2        2          GE1/0/11       poe enable
                                       GE1/0/12       poe max-power 14000
 ---  2 poe-profile(s) created, 8 port(s) applied  ---
```

# Display the information of the PoE configuration file with index number 1.

```
<Sysname> display poe-profile index 1
 Poe-profile     Index   ApplyNum  Interface   Configuration
 forIPphone      1        6          GE1/0/5        poe enable
                                       GE1/0/6        poe priority critical
                                       GE1/0/7
                                       GE1/0/8
                                       GE1/0/9
                                       GE1/0/10
 ---  6 port(s) applied  ---
```

# Display the information of PoE configuration file **forIPphone**.

```
<Sysname> display poe-profile name AA
 Poe-profile     Index   ApplyNum  Interface   Configuration
 forIPphone      1        6          GE1/0/5        poe enable
                                        GE1/0/6        poe priority critical
                                        GE1/0/7
                                        GE1/0/8
                                        GE1/0/9
                                        GE1/0/10
 ---  6 port(s) applied  ---
```

Table 54 Command output

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax

display poe-profile interface *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display poe-profile interface** to display all information of the configurations and applications of the PoE configuration file that currently takes effect on the specified PoE interface.

Examples

# Display all information of the configurations and applications of the current PoE configuration file applied to GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
 Poe-profile     Index   ApplyNum  Interface   Current Configuration
 forIPphone      1        6          GE1/0/1      poe enable
                                                      poe priority critical
```

Not all the configurations of a PoE configuration file can be applied successfully, so only the configurations that currently take effect on the interface are displayed. For the descriptions for other fields, see Table 53.

poe disconnect

Syntax

poe disconnect { **ac** | **dc** }

undo poe disconnect

View

System view

Default level

2: System level

Parameters

ac: Specifies the PD disconnection detection mode as **ac**.

dc: Specifies the PD disconnection detection mode as **dc**.

Description

Use **poe disconnect** to configure a PD disconnection detection mode.

Use **undo poe disconnect** to restore the default.

The default PD disconnection detection mode is **ac**.

Changing to the PD disconnection detection mode may lead to power-off of some PDs.

Examples

# Set the PD disconnection detection mode to **dc**.

```
<Sysname> system-view
[Sysname] poe disconnect dc
```

poe enable

Syntax

poe enable

undo poe enable

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

None

Description

Use **poe enable** to enable PoE on a PoE interface.

Use **undo poe enable** to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

If a PoE configuration file is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE configuration file is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

Examples

# Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

# Enable PoE on a PoE interface through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe legacy enable

Syntax

poe legacy enable pse *pse-id*

undo poe legacy enable pse *pse-id*

View

System view

Default level

2: System level

Parameters

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe legacy enable** to enable the PSE to detect nonstandard PDs.

Use **undo poe legacy enable** to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Examples

# Enable PSE 7 to detect nonstandard PDs (for a device with multiple PSEs).

```
<Sysname> system-view
[Sysname] poe legacy enable pse 7
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

max-power: Specifies the maximum power in milliwatts allocated to a PoE interface. It is in the range of 1000 to 30000 milliwatts.

Description

Use **poe max-power** to configure the maximum power for a PoE interface.

Use **undo poe max-power** to restore the default.

By default, the maximum power that a PoE interface can supply is 30000 milliwatts.

Examples

# Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

# Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts in the PoE configuration file **abc**.

```
<Sysname> system-view
```

```
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe pd-description

Syntax

poe pd-description *text*

undo poe pd-description

View

PoE interface view

Default level

2: System level

Parameters

text: Describes of the PD connected to a PoE interface, a string of 1 to 80 characters.

Description

Use **poe pd-description** to configure a description for the PD connected to a PoE interface.

Use **undo poe pd-description** to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Examples

# Configure the description for the PD connected to GigabitEthernet 1/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax

poe pd-policy priority

undo poe pd-policy priority

View

System view

Default level

2: System level

Parameters

None

Description

Use **poe pd-policy priority** to configure a power management priority policy on the PoE interface.

Use **undo poe pd-policy priority** to restore the default.

By default, no power management priority policy is configured on the PoE interface.

- If the policy is enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system allows the PoE interface to enable the PoE function, but whether the power can be supplied depends on the PoE interface priority.
- If the policy is not enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system will not allow the PoE interface to enable the PoE function.

Examples

# Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe priority

Syntax

poe priority { **critical** | **high** | **low** }

undo poe priority

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

critical: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode. In other words, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description

Use **poe priority** to configure a power priority level for a PoE interface.

Use **undo poe priority** to restore the default.

By default, the power priority of a PoE interface is **low**.

When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.

If a PoE configuration file is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE configuration file is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

Examples

# Set the power priority of GigabitEthernet 1/0/1 to **critical**.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

# Set the power priority of GigabitEthernet 1/0/1 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe update

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

View

System view

Default level

2: System level

Parameters

full: Specifies the upgrade of the PSE processing software in full mode when the software is unavailable.

refresh: Specifies the upgrade of the PSE processing software in refresh mode when the software is available.

filename: Specifies the name of the upgrade file, a string of 1 to 64 characters. This file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe update** to upgrade the PSE processing software online.

To make sure that the PoE function can work correctly after an upgrade, do not use the PSE processing software for a PoE switch on a PoE+ switch, and vice versa.

If none of the PoE commands can be successfully executed, use the full mode to restore the PSE firmware. In any other case, use the full mode only when the refresh mode cannot work correctly.

If you do not provide the *pse-id* argument, the PSEs of all IRF member devices are upgraded.

Examples

# Upgrade the processing software of PSE 7 in service.

```
<Sysname> system-view
[Sysname] poe update refresh 0400_001.S19 pse 7
```

poe utilization-threshold

Syntax

poe utilization-threshold *utilization-threshold-value* **pse** *pse-id*

undo poe utilization-threshold pse *pse-id*

View

System view

Default level

2: System level

Parameters

utilization-threshold-value: Specifies the power alarm threshold in percentage, in the range of 1 to 99.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe utilization-threshold** to configure a power alarm threshold for the PSE.

Use **undo poe utilization-threshold** to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a trap message when the power utilization exceeds the alarm threshold. If the power utilization always stays above the alarm threshold, the system does not send any trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a trap message again.

Examples

# Set the power alarm threshold to 90% for PSE 7.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 7
```

poe-profile

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View

System view

Default level

2: System level

Parameters

profile-name: Specifies the name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Specifies the index number of a PoE configuration file, in the range of 1 to 100.

Description

Use **poe-profile** *profile-name* to create a PoE configuration file and enter PoE-profile view.

Use **undo poe-profile** to delete the specified PoE configuration file.

If no index is specified, the system automatically assigns an index to the PoE configuration file, starting from 1.

If a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

Examples

# Create a PoE configuration file, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view
[Sysname] poe-profile abc 3
```

Cluster management configuration commands

NDP configuration commands

display ndp

Syntax

display ndp [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>,where, *interface-type* is port type and *interface-number* is port number, and &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ndp** to display NDP configuration information, which includes the interval to send NDP packets, the time for the receiving switch to hold NDP information and the information about the neighbors of all ports.

Examples

# Display NDP configuration information.

```
<Sysname> display ndp
Neighbor Discovery Protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet1/0/1
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/2
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/3
```

```
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/4
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/5
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/6
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/7
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/8
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/9
    Status: Enabled, Pkts Snd: 768, Pkts Rvd: 766, Pkts Err: 0

    Neighbor 1:  Aging Time: 159(s)
       MAC Address : 000f-e200-5111
       Host Name   : HP
       Port Name   : GigabitEthernet1/0/32
       Software Ver: V100R001B02D028SP01
       Device Name : HP 5800-24G-PoE+ Switch
       Port Duplex : AUTO
       Product Ver : Alpha 1210
       BootROM Ver : 212

 Interface: GigabitEthernet1/0/10
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/11
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/12
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/13
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/14
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/15
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
```

The rest is omitted.

Table 55 Command output

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the current switch.
Neighbor Discovery Protocol Ver	Version of NDP.
Hello Timer	Interval to send NDP packets.
Aging Timer	Time for the receiving switch to hold NDP information.
Interface	Specified port.
Status	NDP state of a port.
Pkts Snd	Number of the NDP packets sent through the port.
Pkts Rvd	Number of the NDP packets received on the port.
Pkts Err	Number of the error NDP packets received on the port.
Neighbor 1: Aging Time	Aging time of the NDP information of a neighbor switch.
MAC Address	MAC address of a neighbor switch.
Host Name	System name of a neighbor switch.
Port Name	Port name of a neighbor switch.
Software Ver	Software version of the neighbor switch.
Device Name	Switch model of a neighbor switch.
Port Duplex	Port duplex mode of a neighbor switch.
Product Ver	Product version of a neighbor switch.
BootROM Ver	Boot ROM version of a neighbor switch.

ndp enable

Syntax

In Layer 2 Ethernet port view or Layer 2 aggregate interface view:

ndp enable

undo ndp enable

In system view:

ndp enable [**interface** *interface-list*]

undo ndp enable [**interface** *interface-list*]

View

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use **ndp enable** to enable NDP globally or for specified port(s).

Use **undo ndp enable** to disable this feature globally or for specified port(s).

By default, NDP is enabled globally and also on all ports.

Executed in system view, the **ndp enable** command enables NDP for the specified ports. Otherwise, the command enables NDP globally if you provide the **interface** *interface-list* parameter.

Executed in interface view, this command enables NDP only for the current port.

Configured in Layer 2 aggregate interface view, the configuration does not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration takes effect only after the member port quit the aggregation group. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

# Enable NDP globally.

```
<Sysname> system-view
[Sysname] ndp enable
```

# Enable NDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
```

ndp timer aging

Syntax

ndp timer aging *aging-time*

undo ndp timer aging

View

System view

Default level

2: System level

Parameters

aging-time: Time for a switch to keep the NDP packets it receives, which ranges from 5 to 255 seconds.

Description

Use **ndp timer aging** to specify the time that a switch should keep the NDP packets it received from the adjacent switch.

Use **undo timer aging** to restore the default.

By default, the time that a receiving switch should keep the NDP packets is 180 seconds.

The time for the receiving switch to hold NDP packets cannot be shorter than the interval to send NDP packets; otherwise, the NDP table may become unstable.

Related commands: **ndp timer hello**.

Examples

# Configure the time that a receiving switch should keep the NDP packets as 100 seconds.

```
<Sysname> system-view
[Sysname] ndp timer aging 100
```

ndp timer hello

Syntax

ndp timer hello *hello-time*

undo ndp timer hello

View

System view

Default level

2: System level

Parameters

hello-time: Specifies the interval to send NDP packets, which ranges from 5 to 254 seconds.

Description

Use **ndp timer hello** to set the interval to send NDP packets.

Use **undo ndp timer hello** to restore the default.

By default, the interval to send NDP packets is 60 seconds.

The interval for sending NDP packets cannot be longer than the time for the receiving switch to hold NDP packets; otherwise, the NDP table may become unstable.

Related commands: **ndp timer aging**.

Examples

# Set the interval to send NDP packets to 80 seconds.

```
<Sysname> system-view
[Sysname] ndp timer hello 80
```

reset ndp statistics

Syntax

reset ndp statistics [**interface** *interface-list*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. If you provide this keyword, NDP statistics of the specified port will be cleared; otherwise, NDP statistics of all ports will be cleared.

Description

Use **reset ndp statistics** to clear NDP statistics.

Examples

# Clear NDP statistics of all ports.

```
<Sysname> reset ndp statistics
```

NTDP configuration commands

display ntdp

Syntax

display ntdp [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntdp** to display NTDP configuration information.

Examples

# Display NTDP configuration information.

```
<Sysname> display ntdp
 NTDP is running.
 Hops       : 4
 Timer      : 1 min
 Hop Delay : 100 ms
 Port Delay: 10 ms
 Last collection total time: 92ms
```

Table 56 Command output

Field	Description
NTDP is running	NTDP is enabled globally on the local switch.
Hops	Hop count for topology collection.
Timer	Interval to collect topology information (after the cluster is created).
disable	Indicates that the switch is not a management switch and unable to perform periodical topology collection.
Hop Delay	Delay time for the switch to forward topology collection requests.
Port Delay	Delay time for a topology-collection request to be forwarded through a port.
Last collection total time	Time cost during the last topology collection.

display ntdp device-list

Syntax

display ntdp device-list [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays the detailed switch information collected through NTDP.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntdp device-list** to display the switch information collected through NTDP.

The information displayed may not be that of the latest switch if you do not execute the **ntdp explore** command before using this command.

Related commands: **ntdp explore**.

Examples

# Display switch information collected through NTDP.

```
<Sysname> display ntdp device-list
 MAC             HOP  IP                  Device
 000f-e200-3900  2    192.168.0.138/24    HP 5800-24G-PoE+ Switch
 000f-e200-5806  1    192.168.0.58/24     HP 5800-24G-PoE+ Switch
 000f-e200-5104  0    192.168.0.51/24     HP 5500-24G EI Switch
 000f-e200-5111  1    192.168.0.52/24     HP 5800AF-48G Switch
 000f-e200-5600  2    192.168.0.56/24     HP 5800-24G Switch
 000f-e200-0000  2    192.168.0.137/24    HP 5800-24G Switch
 000f-e218-d0d0  2    192.168.0.65/24     HP 5800-24G Switch
```

Table 57 Command output

Field	Description
MAC	MAC address of a switch
HOP	Hops to the collecting switch
IP	IP address and mask length of the management VLAN interface on the switch
Device	Switch model

# Display detailed switch information collected through NTDP.

```
<aaa_0.Sysname> display ntdp device-list verbose
 Hostname   : aaa_1.Sysname
 MAC        : 000f-e200-5806
 Device     : HP 5800-24G-PoE+ Switch
 IP         : 192.168.0.58/24
 Version    :
  HP Comware Platform Software
  Comware Software Version 5.20 Alpha 1210
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP 5800-24G-PoE+ Switch V100R001B02D028SP01

--------------------------------------------------------------------
 Hop        : 3
 Cluster    :  Member device of cluster aaa , Administrator MAC: 000f-e227-afdb
 Peer Hostname  : aaa_10.HP
 Peer MAC       : 000f-e200-5111
 Peer Port ID   : GigabitEthernet1/0/26
 Native Port ID : GigabitEthernet1/0/11
 Speed          : 100
 Duplex         : FULL
```

Table 58 Command output

Field	Description
Hostname	System name of the switch.
MAC	MAC address of the switch.
Device	Switch model.
IP	IP address and subnet mask length of the management VLAN interface on the switch.
Version	Version information.
Hop	Hops from the current switch to the switch that collects topology information.

Field	Description
Cluster	Role of the switch in the cluster: - **Member switch of cluster aaa**—A member switch of the cluster **aaa**. - **Administrator switch of cluster aaa**—The management switch of the cluster **aaa**. - **Candidate switch**—A candidate switch of cluster **aaa**. - **Independent switch**—The switch is connected to the cluster, but it has not joined the cluster. This may be because the cluster function is not enabled on the switch.
Administrator MAC	MAC address of the management switch.
Peer Hostname	System name of a neighbor switch.
Peer MAC	MAC address of a neighbor switch.
Peer Port ID	Name of the peer port connected to the local port.
Native Port ID	Name of the local port to which a neighbor switch is connected.
Speed	Speed of the local port to which a neighbor switch is connected.
Duplex	Duplex mode of the local port to which a neighbor switch is connected.

display ntdp single-device

Syntax

display ntdp single-device mac-address *mac-address* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

mac-address: MAC address of the switch, in the format H-H-H.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntdp single-device mac-address** to view detailed NTDP information about a specified switch.

Examples

# Display detailed NTDP information about the switch with a MAC address of 00E0-FC00-5111.

```
<Sysname> display ntdp single-device mac-address 00e0-fc00-5111
```

```
 Hostname   : aaa_1.Sysname
 MAC        : 00e0-fc00-5111
 Device     : HP 5800-24G-PoE+ Switch
 IP         : 192.168.0.58/24
 Version    :
  HP Comware Platform Software
  Comware Software Version 5.20 Alpha 1210
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP 5800-24G-PoE+ Switch V100R001B02D028SP01

--------------------------------------------------------------------
 Hop        : 0
 Cluster    :  Administrator device of cluster aaa
 Peer Hostname   : aaa_10.Sysname
 Peer MAC        : 000f-e200-5111
 Peer Port ID    : GigabitEthernet1/0/5
 Native Port ID : GigabitEthernet1/0/22
 Speed           : 1000
 Duplex          : FULL
```

Table 59 Command output

Field	Description
Hostname	System name of the switch.
MAC	MAC address of the switch.
Device	Switch model.
IP	IP address and subnet mask length of the management VLAN interface on the switch.
Version	Version information.
Hop	Hops from the current switch to the switch that collects topology information.
Cluster	Role of the switch in the cluster: • **Member switch of cluster aaa**—A member switch of the cluster **aaa**. • **Administrator switch of cluster aaa**—The management switch of the cluster **aaa**. • **Candidate switch**—A candidate switch of cluster **aaa**. • **Independent switch**—The switch is connected to the cluster, but it has not joined the cluster. This may be because the cluster function is not enabled on the switch.
Administrator MAC	MAC address of the management switch.
Peer Hostname	Host name of a neighbor switch.
Peer MAC	MAC address of a neighbor switch.
Peer Port ID	Name of the peer port connected to the local port.
Native Port ID	Name of the local port to which a neighbor switch is connected.
Speed	Speed of the local port to which a neighbor switch is connected.
Duplex	Duplex mode of the local port to which a neighbor switch is connected.

ntdp enable

Syntax

ntdp enable

undo ntdp enable

View

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ntdp enable** to enable NTDP globally or for specified port(s).

Use **undo ntdp enable** to disable NTDP globally or for specified port(s).

By default, NTDP is enabled globally and on all ports.

- Executed in system view, the command enables global NTDP; executed in interface view, the command enables NTDP of the current port.
- Configured in Layer 2 aggregate interface view, the configuration does not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration takes effect only after the member port quit the aggregation group. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

# Enable NTDP globally.

```
<Sysname> system-view
[Sysname] ntdp enable
```

# Enable NTDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntdp enable
```

ntdp explore

Syntax

ntdp explore

View

User view

Default level

2: System level

Parameters

None

Description

Use **ntdp explore** to start topology information collection manually.

Examples

# Start topology information collection manually.

```
<Sysname> ntdp explore
```

ntdp hop

Syntax

ntdp hop *hop-value*

undo ntdp hop

View

System view

Default level

2: System level

Parameters

hop-value: Specifies the maximum hop count for collecting topology information, which ranges from 1 to 16.

Description

Use **ntdp hop** to set the maximum hop count for collecting topology information.

Use **undo ntdp hop** to restore the default.

By default, the maximum hop count is 3.

This command is only applicable to the topology-collecting switch. A bigger number of hops requires more memory of the topology-collecting switch.

Examples

# Set the hop count for topology information collection to 5.

```
<Sysname> system-view
[Sysname] ntdp hop 5
```

ntdp timer

Syntax

ntdp timer *interval*

undo ntdp timer

View

System view

Default level

2: System level

Parameters

interval: Specifies the interval (in minutes) to collect topology information, which ranges from 0 to 65535. A value of 0 means not to collect topology information.

Description

Use **ntdp timer** to configure the interval to collect topology information.

Use **undo ntdp timer** to restore the default.

By default, the interval to collect topology information is 1 minute.

The management switch can start to collect topology information only after the cluster is set up.

Examples

# Set the interval to collect topology information to 30 minutes.

```
<Sysname> system-view
[Sysname] ntdp timer 30
```

ntdp timer hop-delay

Syntax

ntdp timer hop-delay *delay-time*

undo ntdp timer hop-delay

View

System view

Default level

2: System level

Parameters

delay-time: Specifies the delay time (in milliseconds) for a switch receiving topology-collection requests to forward them through its first port. This argument ranges from 1 to 1000.

Description

Use **ntdp timer hop-delay** to set the delay time for the switch to forward topology-collection requests through the first port.

Use **undo ntdp timer hop-delay** to restore the default delay time.

By default, the delay time for the switch to forward topology-collection requests through the first port is 200 ms.

Examples

# Set the delay time for the switch to forward topology-collection requests through the first port to 300 ms.

```
<Sysname> system-view
[Sysname] ntdp timer hop-delay 300
```

ntdp timer port-delay

Syntax

ntdp timer port-delay *delay-time*

undo ntdp timer port-delay

View

System view

Default level

2: System level

Parameters

delay-time: Specifies the delay time (in milliseconds) for a switch to forward a topology-collection request through its successive ports, which ranges from 1 to 100.

Description

Use **ntdp timer port-delay** to set the delay time for a switch to forward a received topology-collection request through its successive ports.

Use **undo ntdp timer port-delay** to restore the default delay time.

By default, the delay time for a switch to forward a received topology-collection request through its successive ports is 20 ms.

Examples

# Set the delay time for the switch to forward topology-collection requests through the successive ports to 40 ms.

```
<Sysname> system-view
[Sysname] ntdp timer port-delay 40
```

Cluster configuration commands

add-member

Syntax

add-member [*member-number*] **mac-address** *mac-address* [**password** *password*]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the member assigned to the candidate switch to be added to a cluster, in the range of 1 to 255.

mac-address: Specifies the MAC address of the candidate switch (in hexadecimal form of H-H-H).

password: Specifies the password of the candidate switch, which is a string of 1 to 16 characters. The password is required when you add a candidate switch to a cluster. However, this argument is not needed if the candidate switch is not configured with a super password.

Description

Use **add-member** to add a candidate switch to a cluster.

This command can be executed only on the management switch.

When you add a candidate switch to a cluster, if you do not assign a number to the switch, the management switch automatically assigns a usable number to the newly added member switch.

After a candidate switch joins the cluster, its level 3 password is replaced by the super password of the management switch in cipher text.

Examples

# Add a candidate switch to the cluster on the management switch, setting the number to 6. (Assume that the MAC address and user password of the candidate switch are 00E0-FC00-35E7 and 123456 respectively.)

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] add-member 6 mac-address 00e0-fc00-35e7 password 123456
```

administrator-address

Syntax

administrator-address *mac-address* **name** *cluster-name*

undo administrator-address

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the MAC address of the management switch (in hexadecimal form of H-H-H).

cluster-name: Specifies the name of an existing cluster. It is a string of 1 to 8 characters, which can only be letters, numbers, hyphen (-), and underline (_).

Description

Use **administrator-address** to add a candidate switch to a cluster.

Use **undo administrator-address** to remove a member switch from the cluster.

By default, a switch belongs to no cluster.

The **administrator-address** command is applicable only on candidate switches, while the **undo administrator-address** command is applicable only on member switches.

To remove a cluster member from a cluster, use the **delete-member** command on the management switch.

Examples

# Remove a member switch from the cluster on the member switch.

```
<aaa_1.Sysname> system-view
[aaa_1.Sysname] cluster
[aaa_1.Sysname-cluster] undo administrator-address
```

auto-build

Syntax

auto-build [**recover**]

View

Cluster view

Default level

2: System level

Parameters

recover: Automatically reestablishes communication with all the member switches.

Description

Use **auto-build** to establish a cluster automatically.

- This command can be executed on a candidate switch or the management switch.
- If you execute this command on a candidate switch, you will be required to enter the cluster name to build a cluster. Then the system will collect candidates and add the collected candidates into the cluster automatically.
- If you execute this command on the management switch, the system will collect candidates directly and add them into the cluster automatically.
- The **recover** keyword is used to recover a cluster. Using the **auto-build recover** command, you can find the members that are currently not in the member list and add them to the cluster again.
- Make sure that NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use the **ntdp hop** command in system view to modify the collection range.
- If a member is configured with a super password different from the super password of the management switch, it cannot be automatically added to the cluster.

Examples

# Establish a cluster automatically on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] auto-build
 Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
n
 Please input cluster name:test
 Collecting candidate list, please wait...

Candidate list:
 Name                            Hops  MAC Address     Device
 HP                              1     000f-e200-a0b0  HP 5500-24G EI Switch
 HP                              3     000f-e2aa-0000  HP 5800-24G-PoE+ Switch
 HP                              3     000f-e200-7000  HP 5800-24G Switch
 HP                              2     000f-e200-0001  HP 5800-24G-PoE+ Switch

 Processing...please wait
 Cluster auto-build Finish!
 4 member(s) added successfully.

[test_0.Sysname-cluster]
```

Table 60 Command output

Field	Description
Restore topology from local flash file,for there is no base topology. (Please confirm in 30 seconds, default No). (Y/N)	Whether to restore the topology information of the cluster from the Flash of the current switch. If there was once a cluster on your network and the standard topology information has been saved to the switch, you can select to restore the standard topology information. For more information about saving the standard topology information, see the **topology accept** and **topology save-to** commands.

# Establish a cluster automatically on the management switch and select to restore the standard topology from the local Flash.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] auto-build
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
y

  Begin get base topology file from local flash......
  Get file OK
  Begin build base topology from file......
  Finish building base topology from file
  Begin build blacklist from file......
  Finish building blacklist from file

 Please input cluster name:test
 Collecting candidate list, please wait...

 Candidate list:

 Name                            Hops  MAC Address     Device
 HP                              1     000f-e200-a0b0  HP 5500-24G EI Switch
 HP                              3     000f-e2aa-0000  HP 5800-24G-PoE+ Switch
 HP                              3     000f-e200-7000  HP 5800-24G Switch
 HP                              2     000f-e200-0001  HP 5800-24G-PoE+ Switch

 Processing...please wait
 Cluster auto-build Finish!
 4 member(s) added successfully.

[test_0.Sysname-cluster]
```

Table 61 Command output

Field	Description
Begin get base topology file from local flash……	Get the standard topology file from the local Flash, and the file name is **topology.top**.
Begin build base topology from file	Begin to restore topology from the standard topology file.
Begin build blacklist from file	Begin to get blacklist from the standard topology file.

black-list add-mac

Syntax

black-list add-mac *mac-address*

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the MAC address of the switch to be added into the blacklist, in the form of H-H-H.

Description

Use **black-list add-mac** to add a switch to the blacklist.

This command can be executed only on the management switch.

Examples

# Add a switch with the MAC address of 0EC0-FC00-0001 to the blacklist on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] black-list add-mac 0ec0-fc00-0001
```

black-list delete-mac

Syntax

black-list delete-mac { **all** | *mac-address* }

View

Cluster view

Default level

2: System level

Parameters

all: Deletes all switches from the blacklist.

mac-address: Specifies the MAC address of the switch to be deleted from the blacklist, which is in the form of H-H-H.

Description

Use **black-list delete-mac** to delete a switch from the blacklist.

This command can be executed only on the management switch.

Examples

# Delete a switch with the MAC address of 0EC0-FC00-0001 from the blacklist on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] black-list delete-mac 0ec0-fc00-0001
```

# Delete all switches in the blacklist on the management switch.

```
[aaa_0.Sysname-cluster] black-list delete-mac all
```

build

Syntax

build *cluster-name*

undo build

View

Cluster view

Default level

2: System level

Parameters

cluster-name: Specifies the cluster name. It is a string of 1 to 8 characters, which can only be letters, numbers, hyphen (-), and underline (_).

Description

Use **build** to configure the current switch as the management switch and specify a cluster name for it.

Use **undo build** to configure the current management switch as a candidate switch.

By default, the switch is not a management switch.

When executing this command, you will be asked whether to create a standard topology map or not.

This command can only be applied to switches that are capable of being a management switch and are not members of other clusters. The command takes no effect if you execute the command on a switch that is already a member of another cluster. If you execute this command on a management switch, you will replace the cluster name with the one you specify (suppose the new cluster name differs from the original one).

The number of the management switch in the cluster is 0.

Examples

# Configure the current switch as a management switch and specify the cluster name as **aabbcc**.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
[Sysname-cluster] build aabbcc
```

```
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
n
#Apr 26 19:25:52:407 2000 Sysname CLST/4/RoleChange:
OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.
e0.fc.00.58.06 role change, NTDPIndex:0.00.00.00.00.00.e0.fc.00.58.06, Role:1

%Apr 26 19:26:06:941 2000 Sysname CLST/4/LOG:
Member 000f-e200-0000 is joined in cluster aabbcc.

%Apr 26 19:26:07:041 2000 Sysname CLST/4/LOG:
Member 00e0-fc02-2180 is joined in cluster aabbcc.

%Apr 26 19:26:07:702 2000 Sysname CLST/4/LOG:
Member 000f-e218-d0d0 is joined in cluster aabbcc.

%Apr 26 19:26:08:014 2000 Sysname CLST/4/LOG:
Member 000f-cb00-5600 is joined in cluster aabbcc.

%Apr 26 19:26:08:546 2000 Sysname CLST/4/LOG:
Member 000f-e200-0144 is joined in cluster aabbcc.
```

Table 62 Command output

Field	Description
Restore topology from local flash file,for there is no base topology. (Please confirm in 30 seconds, default No). (Y/N)	Whether to restore the topology information of the cluster from the Flash of the current switch. If there was once a cluster on your network and the standard topology information has been saved to the switch, you can select to restore the standard topology information. For more information about saving the standard topology information, see the **topology accept** and **topology save-to** commands.
#Apr 26 19:25:52:407 2000 Sysname CLST/4/RoleChange: OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.e0.fc.00.58.06 role change, NTDPIndex:0.00.00.00.00.00.e0.fc.00.58.06, Role:1	Current switch becomes the management switch in the cluster.
%Apr 26 19:26:06:941 2000 Sysname CLST/4/LOG: Member 000f-e200-0000 is joined in cluster aabbcc.	Switch with a MAC address of **000f-e200-0000** has joined cluster **aabbcc**.

cluster

Syntax

cluster

View

System view

Default level

2: System level

Parameters

None

Description

Use **cluster** to enter cluster view.

Examples

# Enter cluster view

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster]
```

cluster enable

Syntax

cluster enable

undo cluster enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **cluster enable** to enable the cluster function.

Use **undo cluster enable** to disable the cluster function.

By default, the cluster function is enabled.

- When you execute the **undo cluster enable** command on a management switch, you remove the cluster and its members, prevent the switch from functioning as a management switch, and disable the cluster function on the switch
- When you execute the **undo cluster enable** command on a member switch, you disable the cluster function on the switch, and the switch leaves the cluster.
- When you execute the **undo cluster enable** command on a switch that belongs to no cluster, you disable the cluster function on the switch.

Examples

# Enable the cluster function.

```
<Sysname> system-view
[Sysname] cluster enable
```

cluster switch-to

Syntax

cluster switch-to { *member-number* | **mac-address** *mac-address* | **administrator** | **sysname** *member-sysname* }

View

User view

Default level

0: Visit level

Parameters

member-number: Specifies the number of a member switch in a cluster, which ranges from 1 to 255.

mac-address *mac-address*: Specifies the MAC address of a member switch, which is in the format H-H-H.

administrator: Switches from a member switch to the management switch.

sysname *member-sysname*: Specifies the system name of a member switch, a string of 1 to 32 characters.

Description

Use **cluster switch-to** to switch between the management switch and member switches.

Examples

# Switch from the operation interface of the management switch to that of the member switch numbered 6 and then switch back to the operation interface of the management switch.

```
<aaa_0.Sysname> cluster switch-to 6
<aaa_6.Sysname> quit
<aaa_0.Sysname>
```

# Enter the member switch numbered 2 with the system name of **5500-2**. There are two devices named 5500-2, and the member IDs of them are 2 and 3 respectively.

```
<aaa_0.Sysname> cluster switch-to sysname 5500-2
 SN   Device                         MAC Address    Status   Name
 2    HP 5500-24G EI Switch         000f-e2aa-0000 Up       aaa_2.5500-2
 3    HP 5500-24G EI Switch         000f-e200-0001 Up       aaa_3.5500-2
 Please select a member-number to input: 2
Trying ...
Press CTRL+K to abort
Connected ...
******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<aaa_2.5500-2>
```

cluster-local-user

Syntax

cluster-local-user *user-name* [**password** { **cipher** | **simple** } *password*]

undo cluster-local-user *user-name*

View

Cluster view

Default level

1: Monitor level

Parameters

user-name: Specifies the username used for logging in to the switches within a cluster through Web, which is a string of 1 to 55 characters.

password: Specifies the password for logging in to the cluster member devices through Web. If this keyword is not specified, you can log in without a password.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

auth-password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

Description

Use **cluster-local-user** to configure web user accounts in batches.

Use **undo cluster-local-user** to remove the configuration.

The command can be configured once only on the management switch.

Examples

# On the management switch, configure a web user account for the cluster member switches.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-local-user abc password simple 123456
```

cluster-mac

Syntax

cluster-mac *mac-address*

undo cluster-mac

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the multicast MAC address (in hexadecimal in the format H-H-H), which can be 0180-C200-0000, 0180-C200-000A, 0180-C200-0020 through 0180-C200-002F, or 010F-E200-0002.

Description

Use **cluster-mac** to configure the destination MAC address for cluster management protocol packets.

Use **undo cluster-mac** to restore the default.

By default, the destination MAC address for cluster management protocol packets is 0180-C200-000A.

This command can be executed only on the management switch.

Examples

# Set the destination MAC address of the cluster management protocol packets to 0180-C200-0000 on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac 0180-C200-0000
```

cluster-mac syn-interval

Syntax

cluster-mac syn-interval *interval*

View

Cluster view

Default level

2: System level

Parameters

interval: Specifies the interval (in minutes) to send MAC address negotiation broadcast packets, which ranges from 0 to 30. If the interval is set to 0, the management switch does not send broadcast packets to the member switches.

Description

Use **cluster-mac syn-interval** to set the interval for a management switch to send MAC address negotiation broadcast packets for cluster management.

By default, the interval is set to one minute.

This command can be executed only on the management switch.

Examples

# Set the interval for the management switch to send MAC address negotiation broadcast packets for cluster management to two minutes on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac syn-interval 2
```

cluster-snmp-agent community

Syntax

cluster-snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name*]

undo cluster-snmp-agent community *community-name*

View

Cluster view

Default level

1: Monitor level

Parameters

read: Indicates to allow the community's read-only access to MIB objects. The community with read-only authority can only query the switch information.

write: Indicates to allow the community's read-write access to MIB objects. The community with read-write authority can configure the switch information.

community-name: Specifies the community name, which is a string of 1 to 26 characters.

view-name: Specifies the MIB view name, a string of 1 to 32 characters.

Description

Use **cluster-snmp-agent community** to configure an SNMP community shared by a cluster and set its access authority.

Use **undo cluster-snmp-agent community** to remove a specified community name.

The command used to configure the SNMP community with read-only or read-and-write authority can only be executed once on the management switch. This configuration will be synchronized to the member switches in the whitelist, which is equivalent to configuring multiple member switches at one time.

An SNMP community name is retained when a cluster is dismissed or a member switch is removed from the whitelist.

If the same community name as the current one has been configured on a member switch, the current community name will replace the original one.

Examples

# Configure the SNMP community name shared by a cluster as **comaccess** and allow the community's read-only access to MIB objects.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent community read comaccess
```

# Configure the SNMP community name shared by a cluster as **comaccesswr** and allow the community's read-write access to MIB objects.

```
[aaa_0.Sysname-cluster] cluster-snmp-agent community write comacceswr
```

cluster-snmp-agent group v3

Syntax

cluster-snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*]

undo cluster-snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

Cluster view

Default level

1: Monitor level

Parameters

group-name: Specifies the group name, a string of 1 to 32 characters.

authentication: Specifies to authenticate a packet but not to encrypt it.

privacy: Specifies to authenticate and encrypt a packet.

read-view: Specifies the read-only view name, a string of 1 to 32 characters.

write-view: Specifies the read-write view name, a string of 1 to 32 characters.

notify-view: Specifies the view name in which trap messages can be sent. It is a string of 1 to 32 characters.

Description

Use **cluster-snmp-agent group** to configure the SNMPv3 group shared by a cluster and set its access rights.

Use **undo cluster-snmp-agent group** to remove the SNMPv3 group shared by a cluster.

The command can be executed once only on the management switch. This configuration will be synchronized to the member switches in the whitelist, which is equivalent to configuring multiple member switches at one time.

The SNMPv3 group name is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same group name as the current one has been configured on a member switch, the current group name will replace the original one.

Examples

# Create an SNMP group **snmpgroup**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent group v3 snmpgroup
```

cluster-snmp-agent mib-view

Syntax

cluster-snmp-agent mib-view included *view-name oid-tree*

undo cluster-snmp-agent mib-view *view-name*

View

Cluster view

Default level

1: Monitor level

Parameters

included: Includes MIB view.

view-name: Specifies the MIB view name, a string of 1 to 32 characters.

oid-tree: Specifies the MIB subtree. It is a string of 1 to 255 characters, which can only be a variable OID string or variable name string. OID is composed of a series of integers, indicating where a node is in the MIB tree. It can uniquely identify an object in a MIB.

Description

Use **cluster-snmp-agent mib-view** to create or update the MIB view information shared by a cluster.

Use **undo cluster-snmp-agent mib-view** to delete the MIB view information shared by a cluster.

By default, the MIB view name shared by a cluster is ViewDefault, in which the cluster can access an ISO subtree.

This command can be executed once only on the management switch. This configuration will be synchronized to member switches on the whitelist, which is equivalent to configuring multiple member switches at one time.

The MIB view is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same view name as the current one has been configured on a member switch, the current view will replace the original one on the member switch.

Examples

# Create a view including all objects of **mib2**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent mib-view included mib2 1.3.6.1.2.1
```

cluster-snmp-agent usm-user v3

Syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } [**cipher** | **simple**] *auth-password* [**privacy-mode des56** [**cipher** | **simple**] *priv-password*]]

undo cluster-snmp-agent usm-user v3 *user-name group-name*

View

Cluster view

Default level

1: Monitor level

Parameters

user-name: Specifies a username, a string of 1 to 32 characters.

group-name: Specifies an SNMP group name, a string of 1 to 32 characters.

authentication-mode: Enables authentication for the SNMP user.

md5: Specifies HMAC-MD5-96 as the authentication algorithm.

sha: Specifies HMAC-SHA-96 as the authentication algorithm.

cipher*:* Specifies a ciphertext authentication key.

simple*:* Specifies a plaintext authentication key.

auth-password: Specifies the authentication key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

privacy-mode: Enables encryption.

des56: Specifies DES as the encryption protocol.

priv-password: Specifies the privacy key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

Description

Use **cluster-snmp-agent usm-user v3** to add a new user to the SNMPv3 group shared by a cluster.

Use **undo cluster-snmp-agent usm-user v3** to delete the SNMPv3 group user shared by the cluster.

The command can be executed once on the management switch only. This configuration will be synchronized to member switches on the whitelist, which is equal to configuring multiple member switches at one time.

The SNMPv3 group user is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same username as the current one has been configured on a member switch, the current username will replace the original one on the member switch.

Examples

# Add a user **wang** to the SNMP group **snmpgroup**, set the security level to authentication-needed and specify the authentication protocol as HMAC-MD5-96, and specify the authentication password as **pass**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent usm-user v3 wang snmpgroup
authentication-mode md5 pass
```

delete-member

Syntax

delete-member *member-number* [**to-black-list**]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the number of a member switch in a cluster, which ranges from 1 to 255.

to-black-list: Adds the switch removed from a cluster to the blacklist to prevent it from being added to the cluster again.

Description

Use **delete-member** to remove a member switch from the cluster.

This command can be executed only on the management switch.

If you only remove a member switch from the cluster without adding it to the blacklist, the switch will be automatically added to the cluster again.

Examples

# On the management switch, remove the member switch numbered 2 from the cluster and add it to the blacklist.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] delete-member 2 to-black-list
```

display cluster

Syntax

display cluster [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster** to display information about the cluster to which the current switch belongs.

This command can be executed only on the management switch and member switches.

Examples

# Display information about the cluster to which the current switch belongs on the management switch.

```
<aaa_0.Sysname> display cluster
 Cluster name:"aaa"
 Role:Administrator
 Management-vlan:100
 Handshake timer:10 sec
 Handshake hold-time:60 sec
 IP-Pool:1.1.1.1/16
 cluster-mac:0180-c200-000a
 No logging host configured
 No SNMP host configured
 No FTP server configured
 No TFTP server configured

 2 member(s) in the cluster, and 0 of them down.
```

# Display information about the cluster to which the current switch belongs on a member switch.

```
<aaa_1.Sysname> display cluster
 Cluster name:"aaa"
 Role:Member
 Member number:1
 Management-vlan:100
 cluster-mac:0180-c200-000a
 Handshake timer:10 sec
 Handshake hold-time:60 sec

 Administrator device IP  address:1.1.1.1
 Administrator device mac address:00e0-fc00-1d00
 Administrator status:Up
```

Table 63 Command output

Field	Description
Cluster name	Name of the cluster.
Role	Role of the switch in the cluster: • **Administrator**—The current switch is a management switch. • **Member**—The current switch is a member switch.
Member number	Number of the switch in the cluster.
Management-vlan	Management VLAN of the cluster.
Handshake timer	Interval to send handshake packets.
Handshake hold-time	Value of handshake timer.
IP-Pool	Private IP addresses of the member switches in the cluster.
cluster-mac	Multicast MAC address of cluster management packets.
Administrator device IP address	IP address of the management switch.
Administrator device mac address	MAC address of the management switch.
Administrator status	State of the management switch.

display cluster base-topology

Syntax

display cluster base-topology [**mac-address** *mac-address* | **member-id** *member-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

mac-address: Specifies a switch by its MAC address. The system displays the standard topology with the switch as the root.

member-number: Specifies a switch by its number. The system displays the standard topology with the switch as the root.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster topology** to display the standard topology information of a cluster.

You can create a standard topology map when executing the **build** or **auto-build** command, or you can use **topology accept** to save the current topology map as the standard topology map.

This command can be executed only on the management switch.

Examples

# Display the standard topology of a cluster.

```
<aaa_0.Sysname> display cluster base-topology
------------------------------------------------------------
     (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
------------------------------------------------------------
[aaa_0.Sysname:0022-57ad-2cf3]
    |
    └-(P_2)<-->(P_2)[aaa_1.5820X:000f-e200-a0b0]
        |
        ├-(P_2/0/25)<-->(P_3/0/1)[aaa_4.5800-2:000f-e200-0001]
        |   |
        |   ├-(P_3/0/5)<-->(P_1/0/1)[aaa_3.5500-2:000f-e200-7000]
        |   |
        |   └-(P_3/0/3)<-->(P_5/0/3)[aaa_2.5800-3:000f-e2aa-0000]
        |
        └-(P_3/0/15)<-->(P_5/0/1)[aaa_2.5800-3:000f-e2aa-0001]
```

Table 64 Command output

Field	Description
PeerPort	Peer port
ConnectFlag	Connection flag: <-->
NativePort	Local port
SysName	System name of the peer switch
DeviceMac	MAC address of the peer switch

display cluster black-list

Syntax

display cluster black-list [**|** { **begin** | **exclude** | **include** } *regular-expression*]

## View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster black-list** to display the current blacklist of a cluster.

This command can be executed only on the management switch.

Examples

# View the current blacklist of the cluster.

```
<aaa_0.Sysname> display cluster black-list
  Device ID           Access Device ID          Access port
  00e0-fc00-0010      00e0-fc00-3550            GigabitEthernet1/0/1
```

Table 65 Command output

Field	Description
Device ID	ID of the blacklist switch, indicated by its MAC address.
Access Device ID	ID of the switch connected to the blacklist switch, indicated by its MAC address.
Access port	Port connected to the blacklist switch.

display cluster candidates

Syntax

display cluster candidates [**mac-address** *mac-address* | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

## View

Any view

Default level

1: Monitor level

Parameters

mac-address *mac-address*: Specifies the MAC address of a candidate switch, which is in the format H-H-H.

verbose: Displays the detailed information about a candidate switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster candidates** to display the information about the candidate switches of a cluster.

The command can be executed only on the management switch.

Examples

# Display information about all the candidate switches.

```
<aaa_0.Sysname> display cluster candidates
 MAC              HOP  IP                   Device
 000f-e200-0001   2                         HP 5800-24G-PoE+ Switch
 000f-e2aa-0000   3                         HP 5800-24G-PoE+ Switch
```

# Display information about a specified candidate switch.

```
<aaa_0.Sysname> display cluster candidates mac-address 000f-e200-0001
 Hostname   : 5800-2
 MAC        : 000f-e200-0001
 Device     : HP 5800-24G-PoE+ Switch
 IP         :
```

# Display the detailed information about all the candidate switches.

```
<aaa_0.Sysname> display cluster candidates verbose
 Hostname   : 5800-2
 MAC        : 000f-e200-0001
 Device     : HP 5800-24G-PoE+ Switch
 IP         :

 Hostname   : 5800-3
 MAC        : 000f-e2aa-0000
 Device     : HP 5800-24G-PoE+ Switch
 IP         :
```

Table 66 Command output

Field	Description
Hostname	System name of a candidate switch
MAC	MAC address of a candidate switch
Hop	Hops from a candidate switch to the management switch

Field	Description
IP	IP address of a candidate switch
Device	Model of a candidate switch

display cluster current-topology

Syntax

display cluster current-topology [**mac-address** *mac-address* [**to-mac-address** *mac-address*] | **member-id** *member-number* [**to-member-id** *member-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

member-number: Specifies the number of the switches in a cluster (including the management switch and member switches).

mac-address: Specifies the MAC addresses of the switches in a cluster (including the management switch and member switches).

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster current-topology** to display the current topology information of the cluster.

- If you specify both the **mac-address** *mac-address* and **to-mac-address** *mac-address* arguments, the topology information of the switches that are in a cluster and form the connection between two specified switches is displayed.
- If you specify both the **member-id** *member-number* and **to-member-id** *member-number* arguments, the topology information of the switches that are in a cluster and form the connection between two specified switches is displayed.
- If you specify only the **mac-address** *mac-address* or **member-id** *member-number* argument, the topology information of all the switches in a cluster is displayed, with a specified switch as the root node.

This command can be executed only on the management switch.

Examples

# Display information about the current topology of a cluster.

```
<aaa_0.Sysname> display cluster current-topology
--------------------------------------------------------------------
```

```
     (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
--------------------------------------------------------------------
ConnectFlag:
   <--> normal connect   ---> odd connect   **** in blacklist
   ???? lost device      ++++ new device    -┤├- STP,RRPP discarding
--------------------------------------------------------------------
[aaa_0.Sysname:0022-57ad-2cf3]
    |
    └-(P_2)<-->(P_2)[aaa_1.5820X:000f-e200-a0b0]
        |
        ├-(P_2/0/25)<-->(P_3/0/1)[aaa_3.5800-2:000f-e200-0001]
        |   |
        |   ├-(P_3/0/3)<-->(P_5/0/3)[aaa_2.5800-3:000f-e2aa-0000]
        |   |
        |   └-(P_3/0/5)****(P_1/0/1)[5500:000f-e200-7000]
        |
        └-(P_3/0/15)-┤├-(P_5/0/1)[aaa_4.5800-4:000f-e2aa-0001]
```

Table 67 Command output

Field	Description
PeerPort	Peer port.
ConnectFlag	Connection flag.
NativePort	Local port.
SysName:DeviceMac	System name of the switch.
<--> normal connect	Indicates a normal connection between the switch and the management switch.
--> odd connect	Indicates a unidirectional connection between the switch and the management switch.
**** in blacklist	Indicates the switch is in the blacklist.
???? lost device	Indicates a lost connection between the switch and the management switch.
++++ new device	Indicates that this is a new switch, whose identity is to be recognized by the administrator.
-||- STP discarding	STP is blocked.

A new switch in the topology information is identified based on the standard topology. After you add a switch into a cluster, if you do not use the **topology accept** command to confirm the current topology and save it as the standard topology, this switch is still regarded as a new switch.

display cluster members

Syntax

display cluster members [*member-number* | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

member-number: Specifies the number of the member switch, which ranges from 0 to 255.

verbose: Displays the detailed information about all the switches in a cluster.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display cluster members** to display the information about cluster members.

This command can be executed only on the management switch.

Examples

# Display the information about all the switches in a cluster.

```
<aaa_0.Sysname> display cluster members
 SN   Device                         MAC Address    Status    Name
 0   HP 5120-24G EI Switch w~      000f-e2ad-2cf3  Admin    aaa_0.Sysname
 1   HP 5800-24G Switch            000f-e200-a0b0  Up       aaa_1.5800
 2   HP 5800-24G Switch            000f-e2aa-0000  Up       aaa_2.5800-3
 3   HP 5800-24G Switch            000f-e200-0001  Up       aaa_3.5800-2
```

Table 68 Command output

Field	Description
SN	Number of the cluster member.
Device	Switch model.
MAC Address	MAC address of a switch.
Status	State of a switch: • **up**—The member switch that is up. • **down**—The member that is down. • **deleting**— The member that is being deleted. • **admin**—The management switch.
Name	System name of a switch.

# Display the detailed information about the management switch and all member switches.

```
<aaa_0.Sysname> display cluster members verbose
 Member number:0
```

```
Name:aaa_0.Sysname
Device:HP 5120-24G EI Switch with 2 Interface Slots
MAC Address: 000f-e2ad-2cf3
Member status:Admin
Hops to administrator device:0
IP: 121.1.1.4/16
Version:
 HP Comware Platform Software
 Comware Software Version 5.20 Release 2208
 Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
 HP 5120-24G EI Switch with 2 Interface Slots V200R002B05D025

Member number:1
Name:aaa_1.5800
Device: HP 5800-24G Switch
MAC Address:000f-e200-a0b0
Member status:Up
Hops to administrator device:1
IP: 121.1.1.2/16
Version:
 HP Comware Platform Software
 Comware Software Version 5.20 Release 1211
 Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
 HP 5800-24G Switch V100R001B02D030

Member number:2
Name:aaa_2.5800-3
Device: HP 5800-24G Switch
MAC Address:000f-e2aa-0000
Member status:Up
Hops to administrator device:3
IP:
Version:
 HP Comware Platform Software
 Comware Software Version 5.20 Release 1211
 Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
 HP 5800-24G Switch V100R001B02D030

Member number:3
Name:aaa_3.5800-2
Device: HP 5800-24G Switch
MAC Address:000f-e200-0001
Member status:Up
Hops to administrator device:2
IP:
Version:
 HP Comware Platform Software
 Comware Software Version 5.20 Release 1211
```

```
Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
HP 5800-24G Switch V100R001B02D030
```

Table 69 Command output

Field	Description
Member number	Number of the cluster member.
Name	Name of a member switch, composed of the cluster name and the system name of the member switch, in the format cluster name.systemname. When the management switch type is not consistent with the member switch type, if a user modifies the cluster name on the management switch continuously, the cluster name may appear twice in the cluster member name, for example, "clustername.clustername.systemname". This abnormal case can restore in a period of time.
Device	Switch model.
MAC Address	MAC address of a switch.
Member status	State of a switch.
Hops to administrator device	Hops from the current member switch to the management switch.
IP	IP address of a member switch.
Version	Software version of the current member switch.

ftp-server

Syntax

ftp-server *ip-address* [**user-name** *username* **password** { **simple** | **cipher** } *password*]

undo ftp-server

View

Cluster view

Default level

3: Manage level

Parameters

ip-address: Specifies the IP address of the FTP server.

username: Specifies the username used to log in to the FTP server, a string of 1 to 32 characters.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

auth-password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

Description

Use **ftp-server** to configure a public FTP server (by setting its IP address, username, and password) on the management switch for the member switches in the cluster.

Use **undo ftp-server** to remove the FTP server configured for the member switches in the cluster.

By default, a cluster is not configured with a public FTP server.

The command can be executed only on the management switch.

Examples

# Set the IP address, username and password of an FTP server shared by the cluster on the management switch to be **1.0.0.9**, **ftp**, and **ftp** respectively.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] ftp-server 1.0.0.9 user-name ftp password simple ftp
```

holdtime

Syntax

holdtime *hold-time*

undo holdtime

View

Cluster view

Default level

2: System level

Parameters

hold-time: Specifies the holdtime in seconds, which ranges from 1 to 255.

Description

Use **holdtime** to configure the holdtime of a switch.

Use **undo holdtime** to restore the default.

By default, the holdtime of a switch is 60 seconds.

This command can be executed only on the management switch.

The configuration is valid on all member switches in a cluster.

Examples

# Set the holdtime to 30 seconds on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] holdtime 30
```

ip-pool

Syntax

ip-pool *ip-address* { *mask* | *mask-length* }

undo ip-pool

View

Cluster view

Default level

2: System level

Parameters

ip-address: Specifies the private IP address of the management switch in a cluster.

{ *mask* | *mask-length* }: Specifies the mask of the IP address pool of a cluster. It is an integer or in dotted decimal notation. When it is an integer, it ranges from 1 to 30. A network address can be obtained by ANDing this mask with the private IP address of the administrator switch. The private IP addresses of all member switches in a cluster belong to this network segment.

Description

Use **ip-pool** to configure a private IP address range for cluster members.

Use **undo ip-pool** to remove the IP address range configuration.

By default, no private IP address range is configured for cluster members.

You must configure the IP address range only on the management switch and before establishing a cluster. If a cluster has already been established, you are not allowed to change the IP address range.

For a cluster to work normally, the IP addresses of the VLAN interfaces of the management switch and member switches must not be in the same network segment as that of the cluster address pool.

Examples

# Configure the IP address range of a cluster.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.200.0.1 20
```

logging-host

Syntax

logging-host *ip-address*

undo logging-host

View

Cluster view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of the logging host.

Description

Use **logging-host** to configure a logging host shared by a cluster.

Use **undo logging-host** to remove the logging host configuration.

By default, no logging host is configured for a cluster.

This command can be executed only on the management switch.

You have to execute the **info-center loghost** command in system view first for the logging host you configured to take effect.

For more information about the **info-center loghost** command, see "Information center configuration commands."

Examples

# Configure the IP address of the logging host shared by a cluster on the management switch as 10.10.10.9.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] logging-host 10.10.10.9
```

management-vlan

Syntax

management-vlan *vlan-id*

undo management-vlan

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies the ID of the management VLAN, which ranges from 1 to 4094.

Description

Use **management-vlan** to specify the management VLAN.

Use **undo management-vlan** to restore the default.

By default, VLAN 1 is the management VLAN.

The management VLAN must be specified before a cluster is created. Once a member switch is added to a cluster, the management VLAN configuration cannot be modified. To modify the management VLAN for a switch belonging to a cluster, you need to cancel the cluster-related configurations on the switch, specify the desired VLAN to be the management VLAN, and then re-create the cluster.

For the purpose of security, you are not recommended to configure the management VLAN as the default VLAN ID of the port connecting the management switch and the member switches.

Only when the default VLAN ID of all cascade ports and the port connecting the management switch and the member switch is the management VLAN, can the packets in the management VLAN packets be passed without a tag. Otherwise, you must configure the packets from a management VLAN to pass these ports. For the more information about the configuration procedure, see *Layer 2—LAN Switching Configuration Guide*.

Examples

# Specify VLAN 2 as the management VLAN.

```
<Sysname> system-view
[Sysname] management-vlan 2
```

management-vlan synchronization enable

Syntax

management-vlan synchronization enable

undo management-vlan synchronization enable

View

Cluster view

Default level

1: Monitor level

Parameters

None

Description

Use **management-vlan synchronization enable** to enable the management VLAN auto-negotiation function.

Use **undo management-vlan synchronization enable** to disable the management VLAN auto-negotiation function.

By default, the management VLAN auto-negotiation function is disabled.

Examples

# Enable the management VLAN auto-negotiation function on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] management-vlan synchronization enable
```

nm-interface vlan-interface

Syntax

nm-interface vlan-interface *interface-name*

View

Cluster view

Default level

2: System level

Parameters

interface-name: Specifies the ID of the VLAN interface. The value range is the same as that of the existing VLAN interface ID.

Description

Use **nm-interface vlan-interface** to configure the VLAN interface of the access management switch (including FTP/TFTP server, management host and log host) as the network management interface of the management switch.

Examples

# Configure VLAN-interface 2 as the network management interface.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] nm-interface vlan-interface 2
```

reboot member

Syntax

reboot member { *member-number* | **mac-address** *mac-address* } [**eraseflash**]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the number of the member switch, which ranges from 1 to 255.

mac-address *mac-address*: Specifies the MAC address of the member switch to be rebooted, which is in the format H-H-H.

eraseflash: Deletes the configuration file when the member switch reboots.

Description

Use **reboot member** to reboot a specified member switch.

This command can be executed only on the management switch.

Examples

# Reboot the member switch numbered 2 on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] reboot member 2
```

snmp-host

Syntax

snmp-host *ip-address* [**community-string read** *string1* **write** *string2*]

undo snmp-host

View

Cluster view

Default level

3: Manage level

Parameters

ip-address: Specifies the IP address of an SNMP host.

string1: Specifies the community name of read-only access, a string of 1 to 26 characters.

string2: Specifies the community name of read-write access, a string of 1 to 26 characters.

Description

Use **snmp-host** to configure a shared SNMP host for a cluster.

Use **undo snmp-host** to cancel the SNMP host configuration.

By default, no SNMP host is configured for a cluster.

This command can be executed only on the management switch.

Examples

# Configure a shared SNMP host for the cluster on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] snmp-host 1.0.0.9 community-string read 123 write 456
```

tftp-server

Syntax

tftp-server *ip-address*

undo tftp-server

View

Cluster view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a TFTP server.

Description

Use **tftp-server** to configure a shared TFTP server for a cluster.

Use **undo tftp-server** to cancel the TFTP server of the cluster.

By default, no TFTP server is configured.

This command can be executed only on the management switch.

Examples

# Configure a shared TFTP server on the management switch as 1.0.0.9.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] tftp-server 1.0.0.9
```

timer

Syntax

timer *interval*

undo timer

View

Cluster view

Default level

2: System level

Parameters

interval: Specifies the interval (in seconds) to send handshake packets. This argument ranges from 1 to 255.

Description

Use **timer** to set the interval to send handshake packets.

Use **undo timer** to restore the default.

By default, the interval to send handshake packets is 10 seconds.

This command can be executed only on the management switch.

This configuration is valid for all member switches in a cluster.

Examples

# Configure the interval to send handshake packets as 3 seconds on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] timer 3
```

topology accept

Syntax

topology accept { **all** [**save-to** { **ftp-server** | **local-flash** }] | **mac-address** *mac-address* | **member-id** *member-number* }

undo topology accept { **all** | **mac-address** *mac-address* | **member-id** *member-number* }

View

Cluster view

Default level

2: System level

Parameters

all: Accepts the current cluster topology information as the standard topology information.

mac-address *mac-address*: Specifies a switch by its MAC address. The switch will be accepted to join the standard topology of the cluster.

member-id *member-number*: Specifies a switch by its number. The switch will be accepted to join the standard topology of the cluster. The *member-number* argument represents the number of a cluster member and ranges from 0 to 255.

save-to: Confirms the current topology as the standard topology, and backs up the standard topology on the FTP server or local flash in a file named "topology.top".

Description

Use **topology accept** to confirm the current topology information and save it as the standard topology.

Use **undo topology accept** to delete the standard topology information.

This command can be executed only on the management switch.

The file used to save standard topology on the FTP server or the local Flash is named "topology.top", which includes the information of both blacklist and the whitelist. A blacklist contains the devices that are prohibited from being added to a cluster. A whitelist contains devices that can be added to a cluster.

Examples

# Take the current topology as the standard topology on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology accept all
```

topology restore-from

Syntax

topology restore-from { **ftp-server** | **local-flash** }

View

Cluster view

Default level

2: System level

Parameters

ftp-server: Restores the standard topology information from the FTP server.

local-flash: Restores the standard topology information from the local flash.

Description

Use **topology restore-from** to restore the standard topology information in case the cluster topology information is incorrect.

This command can be executed only on the management switch.

If the stored standard topology is not correct, the switch cannot be aware of it. Therefore, you must make sure that the standard topology is correct.

Examples

# Restore the standard topology on the management switch.

```
<Sysname> system-view
[Sysname] cluster
```

```
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology restore-from local-flash
```

topology save-to

Syntax

topology save-to { **ftp-server** | **local-flash** }

View

Cluster view

Default level

2: System level

Parameters

ftp-server: Saves the standard topology information to the FTP server.

local-flash: Saves the standard topology information to the local flash.

Description

Use **topology save-to** to save the standard topology information to the FTP server or the local flash.

The file used to save the standard topology on the FTP server or the local Flash is named "topology.top", which includes the information of both the blacklist and the whitelist. A blacklist contains the devices that are prohibited from being added to a cluster. A whitelist contains devices that can be added to a cluster.

This command can be executed only on the management switch.

Examples

# Save the standard topology information to the local flash on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology save-to local-flash
```

Stack management configuration commands

display stack

Syntax

display stack [**members**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

members: Displays stack information for the stack members, including the master device and the member devices. This keyword is only available to the master device of a stack.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stack** to display the stack information.

Examples

# Display stack information on the master device.

```
<stack_0.Sysname> display stack
Role: Master
Management VLAN: 1
IP pool: 1.1.1.1/24
Device total number: 3
```

# Display stack information on a member device.

```
<stack_1.Sysname> display stack
Role: Slave
Management VLAN: 1
IP pool: 1.1.1.1/24
Master MAC address: 000f-e200-1000
```

Table 70 Command output

Field	Description
Role	Role of the device in the stack: • Master indicates that the device is the master device of the stack. • Slave indicates that the device is a member device of the stack.
Management VLAN	ID of the management VLAN, where interactive packets of the stack are transmitted to implement the internal communication between the master device and the member devices.
IP pool	Range of the private IP addresses used by the stack.
Device total number	Total number of the devices in the stack, which is displayed on the master device only.
Master MAC address	MAC address of the master device, which is displayed on a member device only.

# Display stack information for all the stack members on the master.

```
<stack_0.Sysname> display stack members
Number: 0
Role: Master
Sysname: stack_0.Sysname
Device type: HP 5120-24G EI Switch with 2 Interface Slots
MAC Address: 000f-e200-1000

Number: 1
Role: Slave
Sysname: stack_1.Sysname
Device type: HP 5120-24G EI Switch with 2 Interface Slots
MAC Address: 000f-e200-2000
```

Table 71 Command output

Field	Description
Number	Sequence number of the device in the stack: • Value 0 indicates that the device is the master device of the stack. • A value other than 0 indicates that the device is a member device and the value is the sequence number of the member device in the stack.
Role	Role of the device in the stack: • Master indicates that the device is the master device of the stack. • Slave indicates that the device is a member device of the stack.
Sysname	Host name of the device.
MAC Address	MAC address of the device.

stack ip-pool

Syntax

stack ip-pool *ip-address* { *mask* | *mask-length* }

undo stack ip-pool

View

System view

Default level

2: System level

Parameters

ip-address: Start IP address of the stack IP address pool.

mask: IP address mask, in dotted decimal notation. The system ANDs the mask with the specified IP address to get a network segment address, which will be the private IP address pool providing IP addresses for the member devices.

mask-length: IP address mask length, based on which a network segment address is calculated, which will be the private IP address pool providing IP addresses for the member devices.

Description

Use **stack ip-pool** to configure a private IP address pool for a stack.

Use **undo stack ip-pool** to restore the default.

By default, no private IP address pool is configured for a stack.

Before creating a stack, you need to configure a private IP address pool for the stack, so that when a member device joins the stack, the master device can assign an available IP address to it automatically.

Examples

# Configure a private IP address pool containing IP addresses from 192.168.1.1 to 192.168.1.255 for a stack.

```
<Sysname> system-view
[Sysname] stack ip-pool 192.168.1.1 24
```

stack role master

Syntax

stack role master

undo stack role master

View

System view

Default level

2: System level

Description

Use **stack role master** to create a stack.

Use **undo stack role master** to remove a stack.

After you execute the **stack role master** command on a stack-supporting device, the device becomes the master device of a stack and automatically adds the devices connected with its stack ports to the stack.

You can remove a stack only on the master device of the stack.

Examples

# Create a stack.

```
<Sysname> system-view
[Sysname] stack role master
[stack_0.Sysname]
```

stack stack-port

Syntax

stack stack-port *stack-port-num* **port** *interface-list*

undo stack stack-port *stack-port-num* **port** *interface-list*

View

System view

Default level

2: System level

Parameters

stack-port-num: Number of stack ports to be configured. The value range varies with the device model.

interface-list: List of Ethernet ports to be configured as stack ports. You can specify multiple Ethernet ports by providing this argument in the format of *interface-list* = { *interface-type interface-number* }&<1-n>, where *interface-type* is the interface type, *interface-number* is the interface number, and &<1-n> indicates that you can specify up to n ports or port lists. The value of n equals that of *stack-port-num*.

Description

Use **stack stack-port** to configure stack ports.

Use **undo stack stack-port** to restore the default.

By default, no stack port is configured.

Examples

# Configure GigabitEthernet 1/0/1 as a stack port.

```
<Sysname> system-view
[Sysname] stack stack-port 1 gigabitethernet 1/0/1
```

stack switch-to

Syntax

stack switch-to *member-id*

View

User view

Default level

2: System level

Parameters

member-id: ID of the member device which you want to switch to. The value range depends on the device model.

Description

Use **stack switch-to** to switch from the master device to a member device.

This command is used to switch from the master device to a member device with the user level unchanged. To switch back, use the **quit** command.

Examples

# Switch from the master device to member device 1.

```
<stack_0.Sysname> stack switch-to 1
<stack_1.Sysname>
```

Index