Table of Contents

1 Login Commands

Login Commands

authentication-mode

Syntax

authentication-mode { **password** | **scheme** [**command-authorization**] | **none** }

View

User interface view

Parameters

none: Specifies not to authenticate users.

password: Authenticates users using the local password.

scheme: Authenticates users locally or remotely using usernames and passwords.

command-authorization: Performs command authorization on TACACS authentication server.

Description

Use the **authentication-mode** command to specify the authentication mode.

- If you specify the **password** keyword to authenticate users using the local password, remember to set the local password using the **set authentication password** command. Otherwise, AUX users can log in to the switch successfully without password, but VTY users will fail the login. VTY users must enter the correct authentication password to log in to the switch.
- If you specify the **scheme** keyword to authenticate users locally or remotely using usernames and passwords, the actual authentication mode, that is, local or remote, depends on other related AAA scheme configuration of the domain.
- If this command is executed with the **command-authorization** keyword specified, authorization is performed on the TACACS server whenever you attempt to execute a command, and the command can be executed only when you pass the authorization. Normally, a TACACS server contains a list of the commands available to different users.

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

Caution

For a VTY user interface, to specify the **none** keyword or **password** keyword for login users, make sure that SSH is not enabled in the user interface. Otherwise, the configuration fails. Refer to the **protocol inbound** command for related configuration.

Note

To improve security and prevent attacks to the unused Sockets, TCP 23 and TCP 22, ports for Telnet and SSH services respectively, will be enabled or disabled after corresponding configurations.

- If the authentication mode is none, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is password, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is scheme, there are three scenarios: when the supported protocol is specified as telnet, TCP 23 will be enabled; when the supported protocol is specified as SSH, TCP 22 will be enabled; when the supported protocol is specified as all, both the TCP 23 and TCP 22 port will be enabled.

Examples

- Example of the password authentication mode configuration

Configure to authenticate users using the local password on the console port, and set the authentication password to **aabbcc** in plain text.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
[Sysname-ui-aux0] set authentication password simple aabbcc
```

After the configuration, when a user logs in to the switch through the console port, the user must enter the correct password.

- Example of the scheme authentication mode configuration

Configure the authentication mode as **scheme** for VTY users logging in through Telnet.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
```

Specify domain **system** as the default domain, and set the scheme authentication mode to **local** for the domain.

```
[Sysname] domain default enable system
[Sysname] domain system
[Sysname-isp-system] scheme local
[Sysname-ui-vty0] quit
```

Configure the local authentication username and password.

```
[Sysname] local-user guest
[Sysname-luser-guest] password simple 123456
[Sysname-luser-guest] service-type telnet level 2
```

After the configuration, when a user logs in to the switch through VTY0, the user must enter the configured username and password.

auto-execute command

Syntax

auto-execute command *text*

undo auto-execute command

View

VTY user interface view

Parameters

text: Command to be executed automatically.

Description

Use the **auto-execute command** command to set the command that is executed automatically after a user logs in.

Use the **undo auto-execute command** command to disable the specified command from being automatically executed.

By default, no command is configured to be executed automatically after a user logs in.

Normally, the **telnet** command is specified to be executed automatically to enable the user to Telnet to a specific network device automatically.

Caution

- The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.
- Before executing the **auto-execute command** command and save your configuration, make sure you can log in to the switch in other modes and cancel the configuration.

Examples

Configure the **telnet** 10.110.100.1 command to be executed automatically after users log in to VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] auto-execute command telnet 10.110.100.1
% This action will lead to configuration failure through ui-vty0. Are you sure?[
Y/N]y
```

After the above configuration, when a user logs onto the device through VTY 0, the device automatically executes the configured command and logs off the current user.

copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

View

System view

Parameters

None

Description

Use the **copyright-info enable** command to enable copyright information displaying.

Use the **undo copyright-info enable** command to disable copyright information displaying.

By default, copyright information displaying is enabled. That is, the copyright information is displayed after a user logs into a switch successfully.

Note that these two commands apply to users logging in through the console port and by means of Telnet.

Examples

Disable copyright information displaying.

```
**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
**************************************************************************

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

After the above configuration, no copyright information is displayed after a user logs in, as shown below.

```
<Sysname>
```

databits

Syntax

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

undo databits

View

AUX user interface view

Parameters

7: Sets the databits to 7.

8: Sets the databits to 8.

Description

Use the **databits** command to set the databits for the user interface.

Use the **undo databits** command to revert to the default databits.

The default databits is 8.

 **Caution**

- This command takes effect on AUX user interfaces only.
- The databits setting on the terminal and that on the device user interface must be the same for communication.

Examples

Set the databits to 7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

display telnet-server source-ip

Syntax

display telnet-server source-ip

View

Any view

Parameters

None

Description

Use the **display telnet-server source-ip** command to display the source IP address configured for the switch operating as the Telnet server. That is, when the switch operates as the Telnet server, the client uses this IP address to log in to the switch.

- If the source IP address or source interface is specified for the switch, this command displays the IP address or the primary IP address of the source interface.
- If neither source IP address nor source interface is specified, 0.0.0.0 is displayed. That is, as long as there is a route between the switch and client, the client can log in to the switch using the IP address of any Layer 3 interface on the switch.

 **Note**

When you use the **display telnet-server source-ip** command to display the source IP address, the primary IP address of an interface will be displayed even if you have specified a secondary IP address of the interface as the source IP address.

Examples

Display the source IP address configured for the switch operating as the Telnet server.

```
<Sysname> display telnet-server source-ip
The source IP you specified is 192.168.1.1
```

display telnet source-ip

Syntax

display telnet source-ip

View

Any view

Parameters

None

Description

Use the **display telnet source-ip** command to display the source IP address configured for the switch operating as the Telnet client. That is, the source IP address of the Telnet service packets sent when the switch operates as the Telnet client to log in to the remote device.

- If the source interface is specified for the switch, this command displays the IP address of the source interface.
- If no source address or source IP interface is specified for the switch, 0.0.0.0 is displayed. That is, the source IP address of Telnet service packets is that of the outbound interface.

Examples

Display the source IP address configured for the switch operating as the Telnet client.

```
<Sysname> display telnet source-ip
The source IP you specified is 192.168.1.1
```

display user-interface

Syntax

display user-interface [*type number* | *number*] [**summary**]

View

Any view

Parameters

type: User interface type, which can be AUX (for AUX user interface) and VTY (for VTY user interface).

number: User interface index. A user interface index can be relative or absolute.

- In relative user interface number scheme, the *type* argument is required. In this case, AUX user interfaces is numbered AUX0; VTY user interfaces are numbered from VTY0 through VTY4.

- In absolute user interface number scheme, the *type* argument is not required. In this case, user interfaces are numbered from 0 to 5.

summary: Displays the summary information about a user interface.

Description

Use the **display user-interface** command to display the information about a specified user interface or all user interfaces. If the **summary** keyword is not specified, this command displays user interface type, absolute/relative user interface index, transmission speed, available command level, authentication mode, and physical position. If the **summary** keyword is specified, this command displays the number and type of the user interfaces, including those that are in use and those that are not in use.

Examples

Display the information about user interface 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi Auth  Int   Super
F 0    AUX 0    9600       -     3     N     -     S

  +    : Current user-interface is active.
  F    : Current user-interface is active and work in async mode.
  Idx  : Absolute index of user-interface.
  Type : Type and relative index of user-interface.
  Privi: The privilege of user-interface.
  Auth : The authentication mode of user-interface.
  Int  : The physical location of UIs.
  Super: The Super authentication mode of UIs.
  A    : Authentication use AAA.
  N    : Current UI need not authentication.
  P    : Authentication use current UI's password.
  S    : Authentication use super password.
```

Table 1-1 display user-interface command output description

Filed	Description
+	The user interface is in use.
F	The user interface operates in asynchronous mode.
Idx	The absolute index of the user interface
Type	User interface type and the relative index
Tx/Rx	Transmission speed of the user interface
Modem	Indicates whether or not a modem is used.
Privi	Available command level
Auth	Authentication mode
Int	Physical position of the user interface

Filed	Description
Super	The authentication mode used for a user to switch from the current lower user level to a higher level, including S, A, SA and AS. S: Super password authentication A: HWTACACS authentication SA: Super password authentication is preferred, with HWTACACS authentication being a backup AS: HWTACACS authentication is preferred, with super password authentication being a backup For details about the four authentication modes, refer to the *CLI* part of the manual.
A	The current user authentication mode is scheme.
N	The current user authentication mode is none.
P	The current user authentication mode is password.
S	Super password authentication

Display the summary information about the user interface.

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

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

Table 1-2 display user-interface summary command output description

Field	Description
User interface type	User interface type: AUX or VTY
0: X/1:UXXX X	0 and 1 represent the least absolute number for AUX user interfaces and VTY user interfaces. “U” and “X” indicate the usage state of an interface: U indicates that the corresponding user interface is used; X indicates that the corresponding user interface is idle. The total number of Us and Xs is the total number of user interfaces that are available.
character mode users. (U)	The number of current users, that is, the number of Us
UI never used. (X)	The number of user interfaces not being used currently, that is, the number of Xs
total UI in use.	The total number of user interfaces being used currently, that is, the total number of users currently logging in to the switch successfully

display users

Syntax

display users [**all**]

View

Any view

Parameters

all: Displays the user information about all user interfaces.

Description

Use the **display users** command to display the login user information about user interfaces, including AUX user interfaces and VTY user interfaces.

If you do not specify the **all** keyword, only the user information about the user interface that is being used is displayed.

Examples

Display the user information about the current user interface.

```
<Sysname> display users
        UI    Delay     Type   Ipaddress       Username        Userlevel
+ 1   VTY 0   00:00:00  TEL    192.168.0.208                       3

 +   : Current operation user.
 F   : Current operation user work in async mode.
```

Table 1-3 display users command output description

Field	Description
UI	The numbers in the left sub-column are the absolute user interface indexes, and those in the right sub-column are the relative user interface indexes.
Delay	The period (in seconds) the user interface idles for.
Type	User type
Ipaddress	The IP address from which the user logs in.
Username	The login name of the user that logs into the user interface.
Userlevel	The level of the commands available to the users logging in to the user interface
F	The information is about the current user interface, and the current user interface operates in asynchronous mode.
+	The user interface is in use.

display web users

Syntax

display web users

View

Any view

Parameters

None

Description

Use the **display web users** command to display the information about the current on-line Web users (management users that log in to the switch through the Web interface).

Examples

Display the information about the current on-line Web users.

```
<Sysname> display web users
ID         Name     Language     Level        Login Time    Last Req. Time
00800003   admin    English      Management   06:16:32      06:18:35
```

Table 1-4 display web users command output description

Field	Description
ID	ID of a Web user
Name	Name of a Web user
Language	Language a Web user uses
Level	Level of a Web user
Login Time	Time when a Web user logs in
Last Req. Time	Time when the latest request is made

free user-interface

Syntax

free user-interface [*type*] *number*

View

User view

Parameters

type: User interface type, which can be AUX (for AUX user interface) and VTY (for VTY user interface).

number: User interface index. A user interface index can be relative or absolute.

- In relative user interface index scheme, the *type* argument is required. In this case, AUX user interfaces is numbered AUX0; VTY user interfaces are numbered from VTY0 through VTY4.

- In absolute user interface index scheme, the *type* argument is not required. In this case, user interfaces are numbered from 0 to 5.

Description

Use the **free user-interface** command to free a user interface. That is, this command tears down the connection between a user and a user interface. Users of the manage level can use this command to control use of other user interfaces.

Multiple users can log in to the system to configure the device simultaneously. In some circumstances, when the administrator wants to make configurations without interruption from the users that have logged in using other user interfaces, the administrator can execute the following commands to release the connections established on the specified user interfaces.

Note that the current user interface that you are actively using for this command cannot be freed.

Examples

The user logging in to the switch through AUX 0, and with the user level of 3 (manage level) releases user interface VTY 0.

```
<Sysname> display users
        UI    Delay     Type   Ipaddress       Username        Userlevel
F 0   AUX 0   00:00:00                                           3
  8   VTY 0   00:01:30  TEL    192.168.0.108   song               2

 +   : Current operation user.
 F   : Current operation user work in async mode.
<Sysname> free user-interface vty 0
Are you sure you want to free user-interface vty0 [Y/N]? y
 [OK]
```

After you perform the above operation, the user connection on user interface VTY0 is torn down. The user in it must log in again to connect to the switch.

header

Syntax

header [**incoming** | **legal** | **login** | **shell**] *text*

undo header { **incoming** | **legal** | **login** | **shell** }

View

System view

Parameters

incoming: Sets the login banner for users that log in through modems. If you specify to authenticate login users, the banner appears after a user passes the authentication. (The session does not appear in this case.)

legal: Sets the authorization banner, which is displayed when a user enters user view.

login: Sets the login banner. The banner set by this keyword is valid only when users are authenticated before they log in to the switch and appears while the switch prompts for user name and password. If a user logs in to the switch through Web, the banner text configured will be displayed on the banner page.

shell: Sets the session banner, which appears after a session is established. If you specify to authenticate login users, the banner appears after a user passes the authentication.

text: Banner to be displayed. If no keyword is specified, this argument is the login banner. You can provide this argument in two ways. One is to enter the banner in the same line as the command (A command line can accept up to 254 characters.) The other is to enter the banner in multiple lines (you can start a new line by pressing Enter,) where you can enter a banner that can contain up to 2000 characters (including the invisible characters such as carriage return). Note that the first character is the beginning character and the end character of the banner. After entering the end character, you can press Enter to exit the interaction.

Description

Use the **header** command to set the banners that are displayed when a user logs into a switch through an AUX or VTY user interface. The login banner is displayed on the terminal when the connection is established. And the session banner is displayed on the terminal if a user successfully logs in.

Use the **undo header** command to disable displaying a specific banner or all banners.

By default, no banner is configured.

Note

This command is valid to users logging in through AUX and VTY user interfaces, without affecting users logging in through the Web interface.

Note the following:

- If you specify any one of the four keywords without providing the *text* argument, the specified keyword will be regarded as the login information.
- The banner configured with the **header incoming** command is displayed after a modem user logs in successfully or after a modem user passes the authentication when authentication is required. In the latter case, the **shell** banner is not displayed.
- The banner configured with the **header legal** command is displayed when you enter the user interface. If password authentication is enabled or an authentication scheme is specified, this banner is displayed before login authentication.
- With password authentication enabled or an authentication scheme specified, the banner configured with the **header login** command is displayed after the banner configured with the **header legal** command and before login authentication.
- The banner configured with the **header shell** command is displayed after a non-modem user session is established.

Examples

Configure banners.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] header login %Welcome to login!%
[Sysname] header shell %
Input banner text, and quit with the character '%'.
```

```
Welcome to shell!%
[Sysname] header incoming %
Input banner text, and quit with the character '%'.
Welcome to incoming!%
[Sysname] header legal %
Input banner text, and quit with the character '%'.
Welcome to legal!%
```

 **Note**

- The character % is the starting/ending character of *text* in this example. Entering % after the displayed text quits the **header** command.
- As the starting and ending character, % is not a part of a banner.

Test the configuration remotely using Telnet. (only when login authentication is configured can the login banner be displayed).

```
**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
**************************************************************************

Welcome to legal!
 Press Y or ENTER to continue, N to exit.
Welcome to login!

Login authentication

Password:

Welcome to shell!
<Sysname>
```

history-command max-size

Syntax

history-command max-size *value*

undo history-command max-size

View

User interface view

Parameters

value: Size of the history command buffer, ranging from 0 to 256 (in terms of commands).

Description

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

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

By default, the history command buffer of each user can contain up to ten commands.

Each user interface has an independent history command buffer, which saves validated history commands of the current user. The size of a history command buffer determines the number of history commands that can be saved. You can use the **display history-command** command, up-arrow key or down-arrow key to display commands saved in the history command buffer.

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

Related commands: **display history-command**.

Examples

Set the size of the history command buffer of AUX 0 to 20 to enable it to store up to 20 commands.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] history-command max-size 20
```

idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

View

User interface view

Parameters

minutes: Number of minutes. This argument ranges from 0 to 35,791.

seconds: Number of seconds. This argument ranges from 0 to 59.

Description

Use the **idle-timeout** command to set the timeout time. The connection to a user interface is terminated if no operation is performed in the user interface within the timeout time.

Use the **undo idle-timeout** command to revert to the default timeout time.

You can use the **idle-timeout** 0 command to disable the timeout function.

The default timeout time is 10 minutes.

Examples

Set the timeout time of AUX 0 to 1 minute.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] idle-timeout 1
```

ip http shutdown

Syntax

ip http shutdown

undo ip http shutdown

View

System view

Parameters

None

Description

Use the **ip http shutdown** command to shut down the WEB Server.

Use the **undo ip http shutdown** command to launch the WEB Server.

By default, the WEB Server is launched.

Note

To improve security and prevent attacks to the unused Sockets, TCP 80 port for HTTP service will be enabled or disabled after corresponding configurations.

- TCP 80 port is enabled only after you use the **undo ip http shutdown** command to enable the Web server.
- If you use the **ip http shutdown** command to disabled the Web server, TCP 80 port is disabled.

Caution

After the Web file is upgraded, you need to use the **boot web-package** command to specify a new Web file or specify a new Web file from the boot menu after reboot for the Web server to operate properly. Refer to the *File System Management* part in this manual for information about the **boot web-package** command.

Examples

Shut down the WEB Server.

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

Launch the WEB Server.

```
[Sysname] undo ip http shutdown
```

lock

Syntax

lock

View

User view

Parameters

None

Description

Use the **lock** command to lock the current user interface to prevent unauthorized operations in the user interface.

After you execute this command, the system prompts you for the password and prompts you to confirm the password. The user interface is locked only when the password entered is the same both times.

To unlock a user interface, press Enter and then enter the password as prompted.

Note that if you set a password containing more than 16 characters, the system matches only the first 16 characters of the password entered for unlocking the user interface. That is, the system unlocks the user interface as long as the first 16 characters of the password entered are correct.

By default, the current user interface is not locked.

Examples

Lock the current user interface.

```
<Sysname> lock
```

Press Enter, enter a password, and then confirm it as prompted. (The password entered is not displayed).

```
Password:
Again:
                  locked !
```

In this case, the user interface is locked. To operate the user interface again, you need to press Enter and provide the password as prompted.

```
Password:
<Sysname>
```

parity

Syntax

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

undo parity

View

AUX user interface view

Parameters

even: Performs even checks.

none: Does not check.

odd: Performs odd checks.

Description

Use the **parity** command to set the check mode of the user interface.

Use the **undo parity** command to revert to the default check mode.

By default, no check is performed.

Caution:

- This command takes effect on AUX user interfaces only.
- The check mode on the terminal and that on the device user interface must be the same for communication.

Examples

Set to perform even checks.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity even
```

protocol inbound

Syntax

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

View

VTY user interface view

Parameters

all: Supports both Telnet protocol and SSH protocol.

ssh: Supports SSH protocol.

telnet: Supports Telnet protocol.

Description

Use the **protocol inbound** command to specify the protocols supported by the user interface.

Both Telnet protocol and SSH protocol are supported by default.

Related commands: **user-interface vty**.

Note

To improve security and prevent attacks to the unused Sockets, TCP 23 and TCP 22 (ports for Telnet and SSH services respectively) will be enabled or disabled after corresponding configurations.

- If the authentication mode is none, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is password, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is scheme, there are three scenarios: when the supported protocol is specified as telnet, TCP 23 will be enabled; when the supported protocol is specified as ssh, TCP 22 will be enabled; when the supported protocol is specified as all, both the TCP 23 and TCP 22 port will be enabled.

Caution

To configure a user interface to support SSH, you need to set the authentication mode to **scheme** for users to log in successfully. If the authentication mode is set to **password** or **none** for login users, the **protocol inbound ssh** command will fail. Refer to the **authentication-mode** command for the related configuration.

Examples

Configure that only SSH protocol is supported in VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] protocol inbound ssh
```

screen-length

Syntax

screen-length *screen-length*

undo screen-length

View

User interface view

Parameters

screen-length: Number of lines the screen can contain. This argument ranges from 0 to 512.

Description

Use the **screen-length** command to set the number of lines the terminal screen can contain.

Use the **undo screen-length** command to revert to the default number of lines.

By default, the terminal screen can contain up to 24 lines.

You can use the **screen-length** 0 command to disable the function to display information in pages.

Examples

Set the number of lines the terminal screen can contain to 20.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] screen-length 20
```

send

Syntax

send { **all** | *number* | *type number* }

View

User view

Parameters

all: Sends messages to all user interfaces.

type: User interface type, which can be AUX (for AUX user interface) and VTY (for VTY user interface).

number: User interface index. A user interface index can be relative or absolute.

- In relative user interface index scheme, the *type* argument is required. In this case, AUX user interfaces is numbered AUX0; VTY user interfaces are numbered from VTY0 through VTY4.
- In absolute user interface index scheme, the *type* argument is not required. In this case, user interfaces are numbered from 0 to 5.

Description

Use the **send** command to send messages to a user interface or all the user interfaces.

Examples

Send “hello” to all user interfaces.

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

The current user interface will receive the following information:

```
<Sysname>

***
***
***Message from vty1 to vty1
***
hello
```

service-type

Syntax

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* }

View

Local user view

Parameters

ftp: Specifies the users to be of FTP type.

lan-access: Specifies the users to be of LAN-access type, which normally means Ethernet users, such as 802.1x users.

ssh: Specifies the users to be of SSH type.

telnet: Specifies the users to be of Telnet type.

terminal: Makes terminal services available to users logging in through the console port.

level *level*: Specifies the user level for Telnet users, Terminal users, or SSH users. The *level* argument ranges from 0 to 3 and defaults to 0.

Description

Use the **service-type** command to specify the login type and the corresponding available command level.

Use the **undo service-type** command to cancel login type configuration.

Commands fall into four command levels: visit, monitor, system, and manage, which are described as follows:

- Visit level: Commands at this level are used to diagnose network and change the language mode of user interface, such as the **ping**, **tracert**, and **language-mode** command. The **telnet** command is also at this level. Commands at this level cannot be saved in configuration files.
- Monitor level: Commands at this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** commands are at monitor level. Commands at this level cannot be saved in configuration files.
- System level: Commands at this level are used to configure services. Commands concerning routing and network layers are at system level. You can utilize network services by using these commands.
- Manage level: Commands at this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are at administration level.

Refer to *CLI* for detailed introduction to the command level.

Examples

Configure commands at level 0 are available to the users logging in using the user name of **zbr**.

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

```
[Sysname-luser-zbr] service-type telnet level 0
```

To verify the above configuration, you can quit the system, log in again using the user name of **zbr**, and then list the available commands, as listed in the following.

```
<Sysname> ?
User view commands:
  cluster   Run cluster command
  display   Display current system information
  nslookup  Query Internet name servers
  ping      Ping function
  quit      Exit from current command view
  super     Set the current user priority level
  telnet    Establish one TELNET connection
  tracert   Trace route function
  undo      Cancel current setting
```

set authentication password

Syntax

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

undo set authentication password

View

User interface view

Parameters

cipher: Specifies to save the local password in cipher text.

simple: Specifies to save the local password in plain text.

password: Password to be set. The password must be in plain text if you specify the **simple** keyword in the **set authentication password** command. If you specify the **cipher** keyword, the password can be in either cipher text or plain text, as described in the following.

- When you enter the password in plain text containing no more than 16 characters (such as 123), the system converts the password to the corresponding 24-character encrypted password.
- When you enter the password in cipher text containing 24 characters, make sure you are aware of the corresponding password in plaintext. For example, the plain text “123456” corresponds to the cipher text “OUM!K%F<+$[Q=^Q`MAF4<1!!”.

Description

Use the **set authentication password** command to set the local password.

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

Note that only plain text passwords are expected when users are authenticated.

Note

By default, password authentication is performed when a user logs in through a modem or Telnet. If no password is set, the user cannot establish a connection with the switch.

Examples

Set the local password of VTY 0 to “123”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] set authentication password simple 123
```

shell

Syntax

shell

undo shell

View

User interface view

Parameters

None

Description

Use the **shell** command to enable terminal services.

Use the **undo shell** command to disable terminal services.

By default, terminal services are disabled in all user interfaces.

Note the following when using the **undo shell** command:

- Terminal services cannot be disabled in AUX user interfaces.
- This command is unavailable in the current user interface.
- The execution of this command requires user confirmation.

Examples

Disable terminal services in VTY 0 through VTY 4 (assuming that you log in through an AUX user interface).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N]y
```

speed

Syntax

speed *speed-value*

undo speed

View

AUX user interface view

Parameters

speed-value: Transmission speed (in bps). This argument can be 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, and 115,200.

Description

Use the **speed** command to set the transmission speed of the user interface.

Use the **undo speed** command to revert to the default transmission speed.

By default, the transmission speed is 9,600 bps.

 **Caution**

- This command takes effect on AUX user interfaces only.
- The transmission speed setting on the terminal and that on the device user interface must be the same for communication.

Examples

Set the transmission speed of the user interface AUX 0 to 115,200 bps.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 115200
```

stopbits

Syntax

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

undo stopbits

View

AUX user interface view

Parameters

1: Sets the stopbits to 1.

1.5: Sets the stopbits to 1.5.

2: Sets the stopbits to 2.

Description

Use the **stopbits** command to set the stopbits of the user interface.

Use the **undo stopbits** command to revert to the default stopbits.

Execute these two commands in AUX user interface view only.

By default, the stopbits is 1.

Note

- The Switch 4200G does not support communication with a terminal emulation program with stopbits set to 1.5.
- Changing the stop bits value of the switch to a value different from that of the terminal emulation utility does not affect the communication between them.

Examples

Set the stop bits to 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 2
```

telnet

Syntax

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

View

User view

Parameters

hostname: Host name of the remote device, a string of 1 to 20 characters.

ip-address: IPv4 address of the remote device.

service-port: Number of the TCP port through which the remote device provides Telnet service. This argument ranges from 0 to 65535, and defaults to 23.

source-interface *interface-type interface-number*: Specifies the type and number of the source interface.

source-ip *ip-address*: Specifies the source IP address.

Description

Use the **telnet** command to Telnet to another device from the current switch to manage the former remotely. You can terminate a Telnet connection by pressing **Ctrl+K** or by executing the **quit** command.

Examples

Telnet from Ethernet switch Switch A to Switch B whose IP address is 129.102.0.1.

```
<SwitchA> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
Connected to 129.102.0.1 ...
******************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
******************************************************************************

<SwitchB>
```

telnet ipv6

Syntax

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

View

User view

Parameters

remote-system: IPv6 address or host name of the remote system. An IPv6 address can be up to 46 characters; a host name is a string of 1 to 20 characters.

-i *interface-type interface-number*: Specifies the outbound interface by interface type and interface number. The outbound interface is required when the destination address is a local link address.

port-number: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535 and defaults to 23.

Description

Use the **telnet ipv6** command to Telnet to a device from the current device to perform remote management operation. You can terminate a Telnet session by pressing **Ctrl+K**.

Example

Telnet to the device with IPv6 address 3001::1.

```
<Sysname> telnet ipv6 3001::1
Trying 3001::1 ...
Press CTRL+K to abort
Connected to 3001::1 ...
******************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.   *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
******************************************************************************
```

```
<Sysname>
```

telnet source-interface

Syntax

telnet source-interface *interface-type interface-number*

undo telnet source-interface

View

System view

Parameters

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

Description

Use the **telnet source-interface** command to specify the source interface for a Telnet client.

Use the **undo telnet source-interface** command to remove the specified source interface.

The source interface can be a loopback interface or a VLAN interface. If the specified interface does not exist, the system prompts that this configuration fails.

With this command configured, when a device logs in to the Telnet server as a Telnet client, the source IP address is the IP address of the specified interface, the login succeeds only when there is a route between the specified source interface and the Telnet server.

Examples

Specify VLAN-interface 2 as the source interface for the Telnet client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] telnet source-interface Vlan-interface 2
```

telnet source-ip

Syntax

telnet source-ip *ip-address*

undo telnet source-ip

View

System view

Parameters

ip-address: IP address to be set.

Description

Use the **telnet source-ip** command to specify the source IP address for a Telnet client.

Use the **undo telnet source-ip** command to remove the source IP address.

With the **telnet source-ip** command configured, the specified IP address functions as the source IP address when a device logs into a Telnet server as a Telnet client, and the login succeeds only when there is a route between the specified source IP address and the Telnet server.

Note that when the **telnet source-ip** command is executed, if the IP address specified is not an IP address of the local device, your configuration fails.

Examples

Set the source IP address to 192.168.1.1 for the Telnet client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] telnet source-ip 192.168.1.1
```

telnet-server source-interface

Syntax

telnet-server source-interface *interface-type interface-number*

undo telnet-server source-interface

View

System view

Parameters

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

Description

Use the **telnet-server source-interface** command to specify the source interface for a Telnet server.

Use the **undo telnet-server source-interface** command to remove the source interface.

The source interface can be a loopback interface or a VLAN interface. If the specified interface does not exist, the system prompts that this configuration fails, and the login succeeds only when there is a route between the Telnet client and the specified source interface.

With the **telnet-server source-interface** command configured, the client can log in to the local device using only the primary IP address of the specified interface.

Examples

Specify VLAN-interface 2 as the source interface for the Telnet server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] telnet source-interface Vlan-interface 2
```

telnet-server source-ip

Syntax

telnet-server source-ip *ip-address*

undo telnet-server source-ip

View

System view

Parameters

ip-address: Source IP address to be set.

Description

Use the **telnet-server source-ip** command to specify the source Telnet server IP address.

Use the **undo telnet-server source-ip** command to remove the source Telnet server IP address.

With the **telnet-server source-ip** command configured, the client can log in to the local device using the specified IP address only, and the login succeeds only when there is a route between the client and specified source IP address.

Note

- If the specified IP address is not an address on the local switch, the system prompts configuration failure.
- If the specified IP address is a secondary IP address of a Layer 3 interface, a client can log in to the switch using only the primary IP address of the interface.

Examples

Specify the source IP address of the Telnet server as 192.168.1.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] telnet-server source-ip 192.168.1.1
```

user-interface

Syntax

user-interface [*type*] *first-number* [*last-number*]

View

System view

Parameters

type: User interface type, which can be AUX (for AUX user interface) and VTY (for VTY user interface).

first-number: User interface index identifying the first user interface to be configured. A user interface index can be relative or absolute.

- In relative user interface index scheme, the *type* argument is required. In this case, AUX user interfaces is numbered AUX0; VTY user interfaces are numbered from VTY0 through VTY4.
- In absolute user interface index scheme, the *type* argument is not required. In this case, user interfaces are numbered from 0 to 5.

last-number: User interface number identifying the last user interface to be configured. The value of this argument must be larger than that of the *first-number* argument.

Description

Use the **user-interface** command to enter one or more user interface views to perform configuration.

Examples

Enter VTY0 user interface.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0]
```

user privilege level

Syntax

user privilege level *level*

undo user privilege level

View

User interface view

Parameters

level: Command level ranging from 0 to 3.

Description

Use the **user privilege level** command to configure the command level available to the users logging in to the user interface.

Use the **undo user privilege level** command to revert to the default command level.

By default, the commands at level 3 are available to the users logging in to the AUX user interface. The commands at level 0 are available to the users logging in to VTY user interfaces.

Commands fall into four command levels: visit, monitor, system, and manage, which are described as follows:

- Visit level: Commands at this level are used to diagnose network, such as the **ping**, **tracert**, and **telnet** command. Commands at this level cannot be saved in configuration files.
- Monitor level: Commands at this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** commands are at monitor level. Commands at this level cannot be saved in configuration files.
- System level: Commands at this level are used to configure services. Commands concerning routing and network layers are at system level. You can utilize network services by using these commands.
- Manage level: Commands at this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are at administration level.

Refer to *CLI Configuration* for information about command level.

Examples

Configure that commands at level 1 are available to the users logging in to VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 1
```

You can verify the above configuration by Telnetting to VTY 0 and displaying the available commands, as listed in the following.

```
<Sysname> ?
User view commands:
  cluster          Run cluster command
  debugging        Enable system debugging functions
  display          Display current system information
  nslookup         Query Internet name servers
  ping             Ping function
  quit             Exit from current command view
  reset            Reset operation
  send             Send information to other user terminal interfaces
  super            Set the current user priority level
  telnet           Establish one TELNET connection
  terminal         Set the terminal line characteristics
  tracert          Trace route function
  undo             Cancel current setting
```

CLI Configuration Commands

command-privilege level

Syntax

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

undo command-privilege view *view command*

View

System view

Parameters

level *level*: Command level to be set, in the range of 0 to 3.

view *view*: CLI view. It can be any CLI view that the Ethernet switch supports. The Switch 4200G supports only the CLI views listed in Table 1-5:

Table 1-5 Available CLI views for the *view* argument

CLI view	Description
acl-adv	Advanced ACL view
acl-basic	Basic ACL view
acl-ethernetframe	Layer 2 ACL view

CLI view	Description
acl-user	IPv6 ACL view
aux	Aux 1/0/0 port view, that is, console port view
cluster	Cluster view
ftp-client	FTP client view
gigabitethernet	GigabitEthernet port view
hwtacacs	HWTACACS view
isp	ISP domain view
loopback	Loopback interface view
luser	Local user view
mst-region	MST region view
mtlk-group	Monitor link group view
null	NULL interface view
peer-key-code	Public key editing view
peer-public-key	Public key view
poe-profile	PoE profile view
qinq	QinQ view
qos-profile	QoS profile view
radius-template	RADIUS scheme view
remote-ping	Remote-ping test group view
shell	User view
smlk-group	Smart link group view
system	System view
tengigabitethernet	10 Gigabit Ethernet port view
user-interface	User interface view
vlan	VLAN view
vlan-interface	VLAN interface view

command: Command for which the level is to be set.

Description

Use the **command-privilege level** command to set the level of a specified command in a specified view.

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

Commands fall into four levels: visit (level 0), monitor (level 1), system (level 2), and manage (level 3). The administrator can change the level of a command as required. For example, the administrator can change a command from a higher level to a lower level so that the lower level users can use the command.

The default levels of commands are described in the following table:

Table 1-6 Default levels of commands

Level	Name	Command
0	Visit level	Commands used to diagnose network, such as **ping**, **tracert**, and **telnet** commands.
1	Monitor level	Commands used to maintain the system and diagnose service fault, such as **debugging**, **terminal** and **reset** commands.
2	System level	All configuration commands except for those at the manage level.
3	Manage level	Commands associated with the basic operation modules and support modules of the system, such as file system, FTP/TFTP/XMODEM downloading, user management, and level setting commands.

Note that:

- You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.
- When you change the level of a command with multiple keywords or arguments, you should input the keywords or arguments one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect. The values of the arguments should be within the specified ranges.
- When you configure the **undo command-privilege view** command, the value of the *command* argument can be an abbreviated form of the specified command, that is, you only need to enter the keywords at the beginning of the command. For example, after the **undo command-privilege view system ftp** command is executed, all commands starting with the keyword **ftp** (such as **ftp server acl**, **ftp server enable**, and **ftp timeout**) will be restored to the default level; if you have modified the command level of commands **ftp server enable** and **ftp timeout**, and you want to restore only the **ftp server enable** command to its default level, you should use the **undo command-privilege view** system ftp server command.
- If you modify the command level of a command in a specified view from the default command level to a lower level, remember to modify the command levels of the **quit** command and the corresponding command that is used to enter this view. For example, the default command level of commands **interface** and **system-view** is 2 (system level); if you want to make the **interface** command available to the users with the user privilege level of 1, you need to execute the following three commands: **command-privilege level** 1 **view** shell system-view, **command-privilege level** 1 **view** system interface gigabitethernet 1/0/1, and **command-privilege level** 1 **view** system quit, so that the login users with the user privilege level of 1 can enter system view, execute the **interface ethernet** command, and then return to user view.

Examples

Set the level of the **tftp get** command in user view (shell) to 0, and configure the keywords or arguments one by one in the order they appear in the **tftp get** command syntax.

```
[Sysname] command-privilege level 0 view shell tftp
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm
```

Restore the default level of the **tftp get** command. To restore the default levels of the commands starting with the **tftp** keyword, you only need to specify the **tftp** keyword.

```
[Sysname] undo command-privilege view shell tftp
```

display history-command

Syntax

display history-command

View

Any view

Parameters

None

Description

Use the **display history-command** command to display the history commands of the current user, so that the user can check the configurations performed formerly.

History commands are those commands that were successfully executed recently and saved in the history command buffer. You can set the size of the buffer by the **history-command max-size** command. When the history command buffer is full for that user, the earlier commands will be overwritten by the new ones.

By default, the CLI can save 10 history commands for each user.

Related commands: **history-command max-size** in login module.

Examples

Display the history commands of the current user.

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

super

Syntax

super [*level*]

View

User view

Parameters

level: User level, in the range of 0 to 3.

Description

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

Executing this command without the *level* argument will switch the current user level to level 3 by default.

Note that:

- Users logged into the switch fall into four user levels, which correspond to the four command levels respectively. Users at a specific level can only use the commands at the same level or lower levels.
- You can switch between user levels after logging into a switch successfully. The high-to-low user level switching is unlimited. However, the low-to-high user level switching requires the corresponding authentication. The authentication mode can be set through the **super authentication-mode** command.
- For security purpose, the password entered is not displayed when you switch to another user level. You will remain at the original user level if you have tried three times but failed to enter the correct authentication information.

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

Examples

Switch from the current user level to user level 3, using super password authentication.

```
<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
```

Switch from the current user level to level 3, using HWTACACS authentication.

```
<Sysname> super 3
 Username: user@system
 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 { **super-password** | **scheme** }*****

undo super authentication-mode

View

User interface view

Parameters

super-password: Adopts super password authentication for low-to-high user level switching.

scheme: Adopts Huawei terminal access controller access control system (HWTACACS) authentication for low-to-high user level switching.

Description

Use the **super authentication-mode** command to specify the authentication mode used for low-to-high user level switching.

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

By default, super password authentication is adopted for low-to-high user level switching.

Note that, the two authentication modes, super password authentication and HWTACACS authentication, are available at the same time to provide authentication redundancy. When both the two authentication modes are specified, the order to perform the two types of authentication is determined by the order in which they are specified, as described below.

- If the **super authentication-mode super-password scheme** command is executed to specify the authentication mode for user level switching, the super password authentication is preferred and the HWTACACS authentication mode is the backup.
- If the **super authentication-mode scheme super-password** command is executed to specify the authentication mode for low-to-high user level switching, the HWTACACS authentication is preferred and the super password authentication mode is the backup.
- When both the super password authentication and the HWTACACS authentication are specified, the device adopts the preferred authentication mode first. If the preferred authentication mode cannot be implemented (for example, the super password is not configured or the HWTACACS authentication server is unreachable), the backup authentication mode is adopted.

Examples

Specify HWTACACS authentication as the preferred authentication mode when a VTY 0 user switches from the current level to a higher level, with the super password authentication as the backup authentication mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] super authentication-mode scheme super-password
```

super password

Syntax

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

undo super password [**level** *level*]

View

System view

Parameters

level *level*: User level, in the range of 1 to 3. It is 3 by default.

cipher: Stores the password in the configuration file in ciphered text.

simple: Stores the password in the configuration file in plain text.

password: Password to be set. If the **simple** keyword is used, you must provide a plain-text password, that is, a string of 1 to 16 characters. If the **cipher** keyword is used, you can provide a password in either of the two ways:

- Input a plain-text password, that is, a string of 1 to 16 characters, which will be automatically converted into a 24-character cipher-text password.

- Directly input a cipher-text password, that is, a string of 1 to 24 characters, which must correspond to a plain-text password. For example, The cipher-text password “_(TT8F]Y\5SQ=^Q`MAF4<1!!” corresponds to the plain-text password **1234567**.

Description

Use the **super password** command to set a switching password for a specified user level, which will be used when users switch from a lower user level to the specified user level.

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

By default, no such password is set.

Note that, no matter whether a plain-text or cipher-text password is set, users must enter the plain-text password during authentication.

Examples

Set the switching password for level 3 to **0123456789** in plain text.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] super password level 3 simple 0123456789
```

2 Commands for User Control

Commands for Controlling Logging in Users

acl

Syntax

acl *acl-number* { **inbound** | **outbound** }

undo acl *acl-number* { **inbound** | **outbound** }

View

User interface view

Parameters

acl-number: ACL number. This argument can identify different types of ACLs, as listed below.

- 2000 to 2999, for basic ACLs
- 3000 to 3999, for advanced ACLs
- 4000 to 4999, for Layer 2 ACLs

inbound: Applies the ACL for the users Telnetting to the local switch from the current user interface.

outbound: Applies the ACL for the users Telnetting to other devices from the current user interface. This keyword is unavailable to Layer 2 ACLs.

Description

Use the **acl** command to apply an ACL for Telnet users.

Use the **undo acl** command to cancel the configuration.

By default, no ACL is applied.

Examples

Apply ACL 2000 (a basic ACL) for the users Telnetting to the current switch (assuming that ACL 2000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

free web-users

Syntax

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

View

User view

Parameters

all: Specifies all Web users.

user-id: Web user ID, an eight-digit hexadecimal number.

user-name: User name of the Web user. This argument can contain 1 to 80 characters.

Description

Use the **free web-users** command to disconnect a specified Web user or all Web users by force.

Examples

Disconnect all Web users by force.

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

ip http acl

Syntax

ip http acl *acl-number*

undo ip http acl

View

System view

Parameters

acl-number: ACL number ranging from 2000 to 2999.

Description

Use the **ip http acl** command to apply an ACL to filter Web users.

Use the **undo ip http acl** command to disable the switch from filtering Web users using the ACL.

By default, the switch does not use the ACL to filter Web users.

Examples

Apply ACL 2000 to filter Web users (assuming that ACL 2000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ip http acl 2000
```

snmp-agent community

Syntax

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

undo snmp-agent community *community-name*

View

System view

Parameters

read: Specifies that the community has read-only permission in the specified view.

write: Specifies that the community has read/write permission in the specified view.

community-name: Community name, a string of 1 to 32 characters.

acl *acl-number*: Specifies an ACL number for the community. The *acl-number* argument ranges from 2000 to 2999.

mib-view *view-name*: Sets the name of the MIB view accessible to the community. The *view-name* argument is a string of 1 to 32 characters.

Description

Use the **snmp-agent community** command to set a community name and to enable users to access the switch through SNMP. You can also optionally use this command to apply an ACL to perform access control for network management users.

Use the **undo snmp-agent community** command to cancel community-related configuration for the specified community.

By default, SNMPv1 and SNMPv2c access a switch by community names.

Examples

Set the community name to **h123**, enable users to access the switch in the name of the community (with read-only permission). Apply ACL 2000 for network management users (assuming that ACL 2000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent community read h123 acl 2000
```

snmp-agent group

Syntax

In SNMPv1 and SNMPv2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

In SNMPv3:

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

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

System view

Parameters

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

group-name: Group name. This argument can be of 1 to 32 characters.

authentication: Specifies to authenticate SNMP data without encrypting the data.

privacy: Authenticates and encrypts packets.

read-view: Name of the view to be set to read-only. This argument can be of 1 to 32 characters.

write-view: Name of the view to be set to readable & writable. This argument can be of 1 to 32 characters.

notify-view: Name of the view to be set to a notifying view. This argument can be of 1 to 32 characters.

acl *acl-number*: Specifies an ACL. The *acl-number* argument ranges from 2,000 to 2,999.

Description

Use the **snmp-agent group** command to create an SNMP group. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent group** command to remove a specified SNMP group.

By default, the SNMP group configured through the **snmp-agent group v3** command is not authenticated or encrypted.

Examples

Create an SNMP group named **h123** and apply ACL 2001 for network management users (assuming that basic ACL 2001 already exists).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent group v1 h123 acl 2001
```

snmp-agent usm-user

Syntax

For SNMPv1 and SNMPv2c:

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

For SNMPv3:

snmp-agent usm-user v3 *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **engineid** *engineid-string* | **local** }

View

System view

Parameters

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

user-name: User name, a string of 1 to 32 characters.

group-name: Name of the group to which the user corresponds. This argument is a string of 1 to 32 characters.

cipher: Specifies the authentication or encryption password to be in ciphertext.

authentication-mode: Requires authentication. If this keyword is not provided, neither authentication nor encryption is performed.

md5: Adopts HMAC-MD5 algorithm.

sha: Adopts HMAC-SHA algorithm.

auth-password: Authentication password, a string of 1 to 64 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

privacy: Encrypts packets.

des56: Specifies data encryption standard (DES) for encrypting.

aes128: Specifies advanced encryption standard (AES) for encrypting.

priv-password: Encryption password, a string of 1 to 64 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

acl-number: Basic ACL number, ranging from 2000 to 2999.

local: Specifies local entity users.

engineid-string: Engine ID associated with the user, a string of even number of hexadecimal numbers and comprising of 10 to 64 hexadecimal digits.

Description

Use the **snmp-agent usm-user** command to add a user to an SNMP group. You can also optionally use this command to apply an ACL for network management users.

Use the **undo snmp-agent usm-user** command to remove an SNMP user from the corresponding SNMP group and to remove the ACL configuration on the user.

Examples

Add a user named **aaa** to an SNMP group named **group1**, specify to require authentication, specify the authentication protocol as **HMAC-MD5-96** and authentication password as **123**, and apply ACL 2002 to filter network management users (assuming that ACL 2002 already exists).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent usm-user v3 aaa group1 authentication-mode md5 123 acl 2002
```

Table of Contents

1 Configuration File Management Commands

Note

3com Switch 4200G allows you to input a file path and file name in one of the following ways:

- In universal resource locator (URL) format and starting with “unit1>flash:/”. or “flash:/” This method is used to specify a file in the current Flash memory. For example, the URL of a file named **text.txt** in the root directory of the switch is **unit1>flash:/text.txt** or **flash:/text.txt**.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory. For example, to access file text.txt in the current directory, you can directly input the file name **text.txt** as the file URL

File Attribute Configuration Commands

display current-configuration

Syntax

display current-configuration [**configuration** [*configuration-type*] | **interface** [*interface-type*] [*interface-number*]] [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Parameters

configuration *configuration-type*: Specifies to display non-interface configuration. If *configuration-type* is not specified, all the non-interface configurations are displayed; if *configuration-type* is specified, the specified type of configuration is displayed. The configuration type you can specify is based on your current configuration. For example:

- **acl-adv**: Indicates the advanced Access Control List (ACL) configuration.
- **acl-basic**: Indicates the basic ACL configuration.
- **acl-ethernetframe**: Indicates the Layer 2 ACL configuration
- **remote-ping**: Indicates the remote-ping configuration.
- **isp**: Indicates the internet service provider configuration.
- **radius-template**: Indicates the radius template configuration.
- **system**: Indicates the system configuration.
- **user-interface**: Indicates the user interface configuration.

interface: Displays port/interface configuration.

interface-type: Port/interface type, which can be one of the following: Aux, GigabitEthernet, Ten-GigabitEthernet, Loopback, NULL and VLAN-interface.

interface-number: Port/interface number.

by-linenum: Displays configuration information with line numbers.

|: Uses a regular expression to filter the configuration of the switch to be displayed. By specifying a regular expression, you can locate and query the needed information quickly.

regular-expression: A regular expression, case sensitive. It supports the following match rules:

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays only the lines that match the regular expression.

A regular expression also supports some special characters. For match rules of the special characters, refer to Table 1-1 for details.

Table 1-1 Special characters in regular expression

Character	Meaning	Remarks
^	Starting sign, the string to the right of this character appears only at the beginning of a line.	For example, regular expression **^user** matches lines beginning with **user**, not **Auser**.
$	Ending sign, the string to the left of this character appears only at the end of a line.	For example, regular expression **user$** matches lines ending with **user**, not **userA**.
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, the character to the left of the asterisk should match zero or more consecutive times.	For example, **zo*** can match **z** and **zoo**, and so on, but not **zo**.
+	Plus sign, the character to the left of the plus sign should match one or more consecutive times.	For example, **zo+** can match **zo** and **zoo**, and so on, but not **z**.
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, **1-9** means numbers from 1 to 9 (inclusive); **a-h** means from **a** to **h** (inclusive).
[ ]	Square brackets. Specifies a range of characters, and matches any character in the specified range.	For example, **[1-36A]** can match a string containing any character among 1, 2, 3, 6, and A.
( )	Parenthesis. Specifies a character group. It is usually used with + or *.	For example, **(123A)** means a character group **123A**; **408(12)+** can match 40812 or 408121212. But it cannot match 408. That is, **12** can appear continuously and it must at least appear once.

Description

Use the **display current-configuration** command to display the current configuration of a switch.

After you finish a set of configurations, you can execute the **display current-configuration** command to display the parameters that take effect currently.

Note that:

- Parameters that are the same as the default are not displayed.
- The configured parameter whose corresponding function does not take effect is not displayed.

Related commands: **save**, **reset saved-configuration**, **display saved-configuration**.

Examples

Display configuration information about all the interfaces on the current switch.

```
<Sysname> display current-configuration interface
#
interface Vlan-interface1
 ip address 192.168.0.54 255.255.255.0
#
interface Vlan-interface2
#
interface Vlan-interface3
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1
 voice vlan enable
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface GigabitEthernet1/0/5
#
interface GigabitEthernet1/0/6
#
interface GigabitEthernet1/0/7
#
interface GigabitEthernet1/0/8
#
interface GigabitEthernet1/0/9
#
interface GigabitEthernet1/0/10
#
interface GigabitEthernet1/0/11
#
interface GigabitEthernet1/0/12
#
interface GigabitEthernet1/0/13
 shutdown
#
interface GigabitEthernet1/0/14
 shutdown
#
interface GigabitEthernet1/0/15
 shutdown
```

```
#
interface GigabitEthernet1/0/16
 shutdown
#
interface NULL0
#
return
```

Display the lines that include the strings matching **10*** in the configuration information. (The character ***** means that the character **0** in the string before it can appear multiple times or does not appear.)

```
<Sysname> display current-configuration | include 10*
domain 1
vlan 1 to 3
vlan 10
interface Vlan-interface1
 ip address 192.168.0.91 255.255.255.0
interface Aux1/0/0
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
interface GigabitEthernet1/0/3
interface GigabitEthernet1/0/4
interface GigabitEthernet1/0/5
interface GigabitEthernet1/0/6
interface GigabitEthernet1/0/7
interface GigabitEthernet1/0/8
interface GigabitEthernet1/0/9
interface GigabitEthernet1/0/10
interface GigabitEthernet1/0/11
interface GigabitEthernet1/0/12
interface GigabitEthernet1/0/13
interface GigabitEthernet1/0/14
interface GigabitEthernet1/0/15
interface GigabitEthernet1/0/16
```

Display the configuration information starting with the string **user**.

```
<Sysname> display current-configuration | include ^user
user-interface aux 0
user-interface vty 0 4
```

display current-configuration vlan

Syntax

display current-configuration vlan [*vlan-id*] [**by-linenum**]

View

Any view

Parameters

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

by-linenum: Displays configuration information with line numbers.

Description

Use the **display current-configuration vlan** command to display the current VLAN configuration of the switch.

Without the *vlan-id* argument specified, this command displays configuration information about all the VLANs that exist on the switch.

If there are contiguous VLANs without any configuration, the system combines these VLANs together in the format of *vlan-id* **to** *vlan-id* when displaying the VLAN configuration information.

Related commands: **save**, **reset saved-configuration**, **display saved-configuration**.

Examples

Display the VLAN configuration information of the current switch.

```
<Sysname> display current-configuration vlan
#
vlan 1
#
vlan 100 to 200
#
return
```

display saved-configuration

Syntax

display saved-configuration [**unit** *unit-id*] [**by-linenum**]

View

Any view

Parameters

unit *unit-id*: Specifies the unit ID of a switch. It only can be 1.

by-linenum: Displays configuration information with line numbers.

Description

Use the **display saved-configuration** command to display the initial configuration file of a switch.

Note that:

- If the switch starts up without a configuration file, the system will display that no configuration file exists upon execution of the command.
- If you have saved configuration after the switch starts up, the command displays the last saved configuration.

Related commands: **save**, **reset saved-configuration**, **display current-configuration**.

Examples

Display the initial configuration file of the current switch.

```
<Sysname> display saved-configuration
```

```
#
 sysname Sysname
#
radius scheme system
#
domain system
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.54 255.255.255.0
#LOCCFG. MUST NOT DELETE
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface GigabitEthernet1/0/5
#
interface GigabitEthernet1/0/6
#
interface GigabitEthernet1/0/7
#
interface GigabitEthernet1/0/8
#
interface GigabitEthernet1/0/9
#
interface GigabitEthernet1/0/10
#
interface GigabitEthernet1/0/11
#
interface GigabitEthernet1/0/12
#
interface GigabitEthernet1/0/13
 shutdown
#
interface GigabitEthernet1/0/14
 shutdown
#
interface GigabitEthernet1/0/15
 shutdown
#
```

```
interface GigabitEthernet1/0/16
 shutdown
#TOPOLOGYCFG. MUST NOT DELETE
#GLBCFG. MUST NOT DELETE
#
interface NULL0
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

The configuration information output above in turn is the system configuration, logical interface configuration, physical port configuration, and user interface configuration.

display startup

Syntax

display startup [**unit** *unit-id*]

View

Any view

Parameters

unit *unit-id*: Specifies the unit ID of a switch. It only can be 1.

Description

Use the **display startup** command to display the startup configuration of a switch.

Related commands: **startup saved-configuration**.

Examples

Display the startup configuration file information of the current switch.

```
<Sysname> display startup
UNIT1:
  Current Startup saved-configuration file:          flash:/config.cfg
  Next main startup saved-configuration file:        flash:/config.cfg
  Next backup startup saved-configuration file:      flash:/backup.cfg
  Bootrom-access enable state:                       enabled
```

Table 1-2 Description on the fields of the **display startup** command

Field	Description
Current Startup saved-configuration file	The configuration file used for the current startup
Next main startup saved-configuration file	The main configuration file used for the next startup

Field	Description
Next backup startup saved-configuration file	The backup configuration file used for the next startup
Bootrom-access enable state	Whether you can use the user-defined password to access the Boot ROM: • **enabled** indicates you can access the Boot ROM with the user-defined password. • **disabled** indicates you cannot access the Boot ROM with the user-defined password. For related information, refer to the **startup bootrom-access enable** command in the *File System Management* part of the manual.

display this

Syntax

display this [**by-linenum**]

View

Any view

Parameters

by-linenum: Displays configuration information with line numbers.

Description

Use the **display this** command to display the current configuration performed in the current view. To verify the configuration performed in a view, you can use this command to display the parameters that are valid in the current view.

Note that:

- Effective parameters that are the same as the default are not displayed.
- The configured parameter whose corresponding function does not take effect is not displayed.
- Execution of this command in any user interface view or VLAN view displays the valid configuration parameters in all user interfaces or VLANs.

Related commands: **save**, **reset saved-configuration**, **display saved-configuration**, **display current-configuration**.

Examples

Display the configuration parameters that take effect in all user interface views.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] display this
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
```

```
 user privilege level 3
#
return
```

reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

Parameters

backup: Erases the backup configuration file.

main: Erases the main configuration file.

Description

Use the **reset saved-configuration** command to erase the configuration file saved in the Flash of a switch.

The following two situations exist:

- While the **reset saved-configuration** [**main**] command erases the configuration file with main attribute, it only erases the main attribute of a configuration file having both main and backup attribute.
- While the **reset saved-configuration backup** command erases the configuration file with backup attribute, it only erases the backup attribute of a configuration file having both main and backup attribute.

You may need to erase the configuration file for one of these reasons:

- After you upgrade software, the old configuration file does not match the new software.
- The startup configuration file is corrupted or not the one you need.

Caution

- This command will permanently delete the configuration file from the switch.
- An error occurs when you execute this command if the configuration file to be deleted does not exist.

Related commands: **save**.

Examples

Erase the main configuration file to be used in the next startup.

```
<Sysname> reset saved-configuration main
The saved configuration will be erased.
Are you sure?[Y/N]y
Configuration in flash memory is being cleared.
```

```
Please wait ...
....
 Unit1 reset saved-configuration successfully.
```

save

Syntax

save [*cfgfile* | [**safely**] [**backup** | **main**]]

View

Any view

Parameters

cfgfile: Path name or file name of a configuration file in the Flash, a string of 5 to 56 characters.

safely: Saves the current configuration in the safe mode.

backup: Saves the configuration to the backup configuration file.

main: Saves the configuration to the main configuration file.

Description

Use the **save** command to save the current configuration to a configuration file in the Flash.

When you use this command to save the configuration file,

- If the **main** and **backup** keywords are not specified, the current configuration will be saved to the main configuration file.
- If the *cfgfile* argument is specified, but the file specified by it does not exist, the system will create the file and then save the current configuration to it. The file attribute is neither **main** nor **backup**.
- If the *cfgfile* argument is specified and the file specified by it exists, the system will save the current configuration to the specified file. The file attribute is the original attribute of the file.
- If the *cfgfile* argument is not specified, the system will save the current configuration to the configuration file used for this startup. If the switch starts up without loading the configuration file, the system will save the current configuration with the default name (config.cfg) in the root directory.

The system supports two modes for saving the current configuration file.

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file quicker but is likely to lose the original configuration file if the switch reboots or the power fails during the process.
- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file slower but can retain the original configuration file in the Flash even if the switch reboots or the power fails during the process.

Note

- It is recommended to adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.
- The extension name of the configuration file must be .cfg.

Examples

Save the current configuration to **123.cfg** as the main configuration file for the next startup.

```
<Sysname> save main
The configuration will be written to the device.
Are you sure?[Y/N]y
Please input the file name(*.cfg)(To leave the existing filename
 unchanged press the enter key):123.cfg

Now saving current configuration to the device.
Saving configuration. Please wait...
............
 Unit1 save configuration flash:/123.cfg successfully
```

startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration [**unit** *unit-id*]

View

User view

Parameters

cfgfile: Path name or file name of a configuration file in the Flash, a string of 5 to 56 characters.

backup: Specifies the configuration file to be the backup configuration file.

main: Specifies the configuration file to be the main configuration file.

unit *unit-id*: Specifies a switch by its unit ID. It only can be 1.

Description

Use the **startup saved-configuration** command to specify a configuration file to be the main configuration file or the backup configuration file to be used for the next startup of the switch.

Use the **undo startup saved-configuration** command to specify a switch to use null configuration when it restarts.

Note that: If you execute the **startup saved-configuration** command with neither the **backup** nor the **main** keyword specified, the configuration file identified by the *cfgfile* argument is specified as the main configuration file to be used for the next startup of the switch.

Caution

The configuration file must use **.cfg** as its extension name and the startup configuration file must be saved at the root directory in the Flash of the switch.

Related commands: **display startup**.

Examples

Configure the configuration file named **config.cfg** as the main configuration file to be used for the next startup of the current switch.

```
<Sysname> startup saved-configuration config.cfg main
 Please wait......Done!
```

Table of Contents

1 VLAN Configuration Commands

VLAN Configuration Commands

description

Syntax

description *text*

undo description

View

VLAN view, VLAN interface view

Parameters

text: Case sensitive character string to describe the current VLAN or VLAN interface. Special characters and spaces are allowed.

It has:

- 1 to 32 characters for a VLAN description.
- 1 to 80 characters for a VLAN interface description.

Description

Use the **description** command to configure the description of the current VLAN or VLAN interface. You can use the description to provide information helping identify the devices or network segment attached to the VLAN or VLAN interface, and so on.

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

By default, the description of a VLAN is its VLAN ID, for example **VLAN 0001**; the description of a VLAN interface is its name, for example **Vlan-interface 1 Interface**.

You can display the description of a VLAN or VLAN interface with the **display vlan** or **display interface Vlan-interface** command.

Examples

Configure the description of VLAN 10 as **connect to LAB1**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 10
[Sysname-vlan10] description connect to LAB1
```

Configure the description of VLAN-interface 1 as **gateway of LAB1**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] description gateway of LAB1
```

display interface Vlan-interface

Syntax

display interface Vlan-interface [*vlan-id*]

View

Any view

Parameters

vlan-id: Specifies a VLAN interface number.

Description

Use the **display interface Vlan-interface** command to display information about the specified VLAN interface or all VLAN interfaces already created if no VLAN interface is specified.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the layer 3 communication between different VLANs. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer.

The output of this command shows the state, IP address, description and other information of a VLAN interface. You can use the information to troubleshoot network problems.

Related commands: **interface Vlan-interface**.

Examples

Display information about all existing VLAN interfaces.

```
<Sysname> display interface Vlan-interface 1
Vlan-interface1 current state :UP
Line protocol current state :UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc00-5191
Internet Address is 192.168.0.1/24 Primary
Description : Vlan-interface1 Interface
The Maximum Transmit Unit is 1500
```

Table 1-1 Description on the fields of the **display interface Vlan-interface** command

Field	Description
Vlan-interface1 current state	The state of the VLAN interface, which can be one of the following: • Administratively DOWN: This VLAN interface has been manually disabled with the **shutdown** command. • DOWN: The administrative state of this VLAN interface is up, but its physical state is down. It indicates that the VLAN corresponding to this interface does not contain ports in up state (possibly because the lines have failed). • UP: The administrative and physical states of this VLAN interface are both up.

Field	Description
Line protocol current state	The link layer protocol state of the VLAN interface, which can be one of the following: • DOWN: The protocol state of this VLAN interface is down, usually because no IP address is configured. • UP: The protocol state of this VLAN interface is up.
IP Sending Frames' Format is PKTFMT_ETHNT_2	Format of the frames sent from the VLAN interface. PKTFMT_ETHNT 2 indicates that this VLAN interface sends Ethernet II frames. Refer to the VLAN configuration part in the accompanied operation manual for information about frame formats.
Hardware address	MAC address corresponding to the VLAN interface
Internet Address	IP address corresponding to the VLAN interface
192.168.0.1/24 Primary	Primary IP address of this VLAN interface
Description	Description string of the VLAN interface
The Maximum Transmit Unit	Maximum transmission unit (MTU)

Note

For information about how to configure an IP address for a VLAN interface, refer to the description on the **ip address** command in the *IP Address and Performance Command* part.

display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id*2] | **all** | **dynamic** | **static**]

View

Any view

Parameters

vlan-id1: Specifies the ID of a VLAN of which information is to be displayed, in the range of 1 to 4094.

to *vlan-id2*: In conjunction with *vlan-id1*, define a VLAN range to display information about all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.

all: Displays information about all the VLANs.

dynamic: Displays the number of dynamic VLANs and the ID of each dynamic VLAN. Dynamic VLANs refer to VLANs that are generated through GVRP or those distributed by a RADIUS server.

static: Displays the number of static VLANs and the ID of each static VLAN. Static VLANs refer to VLANs manually created.

Description

Use the **display vlan** command to display information about VLANs. The output shows the ID, type, VLAN interface state and member ports of a VLAN.

If no keyword or argument is specified, the command displays the number of existing VLANs in the system and the ID of each VLAN.

Related commands: **vlan**.

Examples

Display information about VLAN 1.

```
<Sysname> display vlan 1
 VLAN ID: 1
 VLAN Type: static
 Route Interface: configured
 IP Address: 192.168.0.39
 Subnet Mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged   Ports:
  GigabitEthernet1/0/1
 Untagged Ports:
  GigabitEthernet1/0/2
```

Table 1-2 Description on the fields of the **display vlan** command

Field	Description
VLAN ID	VLAN ID.
VLAN Type	VLAN type (dynamic or static).
Route Interface	Indicates whether the VLAN interface of the VLAN is configured with an IP address for routing.
IP Address	IP address of the VLAN interface (available only on a VLAN interface configured with an IP address).
Subnet Mask	Subnet mask of the IP address of the VLAN interface.
Description	Description of the VLAN.
Name	VLAN name.
Tagged Ports	Ports out of which packets are sent tagged.
Untagged Ports	Ports out of which packets are sent untagged.

interface Vlan-interface

Syntax

interface Vlan-interface *vlan-id*

undo interface Vlan-interface *vlan-id*

View

System view

Parameters

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

Description

Use the **interface Vlan-interface** command to create the VLAN interface for a VLAN and enter VLAN interface view.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the layer 3 communication between different VLANs. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer.

Use the **undo interface Vlan-interface** command to delete a VLAN interface.

You can create a VLAN interface only for an existing VLAN and must ensure that the ID of the VLAN interface is the same as the VLAN ID.

You can use the **ip address** command in VLAN interface view (refer to the *IP Address and Performance Command* part for the command description) to configure an IP address for this VLAN interface.

Related commands: **display interface Vlan-interface**.

Examples

Create the VLAN interface for VLAN 1 and enter VLAN-interface 1 view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1]
```

name

Syntax

name *text*

undo name

View

VLAN view

Parameters

text: VLAN name, a description of 1 to 32 characters. It can contain special characters and spaces.

Description

Use the **name** command to assign a name to the current VLAN.

Use the **undo name** command to restore the default VLAN name.

When 802.1x or MAC address authentication is configured on the switch, a RADIUS server may be used to deploy VLANs (either named or numbered) on the ports that have passed authentication. If a named VLAN is deployed, you must use the **name** command to associate the VLAN name with the intended VLAN ID. The name of a VLAN must be unique among all VLANs.

By default, the name of a VLAN is its VLAN ID, **VLAN 0001** for example.

Examples

Specify the name of VLAN 2 as **test vlan**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

shutdown

Syntax

shutdown

undo shutdown

View

VLAN interface view

Parameters

None

Description

Use the **shutdown** command to administratively shut down the VLAN interface.

Use the **undo shutdown** command to bring up the VLAN interface.

By default, a VLAN interface is administratively enabled. In this case, the physical state of the VLAN interface is affected by that of the ports in the VLAN.

- When all the Ethernet ports in the VLAN are down, the VLAN interface of the VLAN is down, that is, disabled.
- When one or more Ethernet ports in the VLAN are up, the VLAN interface of the VLAN is up, that is, enabled.

If you shut down the VLAN interface manually, the administrative state of the VLAN interface will always be down, regardless of the state of the ports in the VLAN.

You can use the **undo shutdown** command to enable a VLAN interface when its related parameters and protocols are configured. When a VLAN interface fails, you can use the **shutdown** command to

disable the interface, and then use the **undo shutdown** command to enable this interface again, which may restore the interface.

Enabling or disabling a VLAN interface does not influence the state of the Ethernet ports belonging to this VLAN.

Related commands: **display interface Vlan-interface**.

Examples

Disable the VLAN-interface2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] shutdown
```

vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

System view

Parameters

vlan-id1: Specifies the ID of the VLAN you want to create or remove, in the range of 1 to 4094.

to *vlan-id2*: In conjunction with *vlan-id1,* specify a VLAN ID range you want to create or remove. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.

all: Creates or removes all existing VLANs except those configured with other functions.

Description

Use the **vlan** command to create VLANs. If you create only one VLAN, you enter the view of the VLAN upon its creation; if the specified VLAN already exists, you enter its VLAN view directly.

Use the **undo vlan** command to remove VLANs.

By default, only VLAN 1 exists in the system.

Caution

- VLAN 1 is the default VLAN and cannot be removed.
- You cannot use the **undo vlan** command to directly remove the VLANs reserved by the protocol, voice VLAN, control VLANs for Smart Link, probe VLANs for remote mirroring, or VLANs used for performing any other features. To remove them, you must remove the associations of them with the features.
- After you use the **undo vlan** command to remove a VLAN functioning as the default VLAN of a trunk or a hybrid port, the configuration of the default VLAN on the trunk port or hybrid port does not change. The port will continue to use the removed VLAN as its default VLAN.

Examples

Create VLAN 5 and enter its VLAN view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 5
[Sysname-vlan5]
```

Remove VLAN 5.

```
[Sysname-vlan5] quit
[Sysname] undo vlan 5
```

Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 4 to 100
Please wait.............. Done.
```

Remove VLAN 2 through VLAN 9 in bulk. VLAN 7 is the voice VLAN.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] undo vlan 2 to 9
 Note:The VLAN kept by protocol, the voice VLAN,  the default VLAN, the management VLAN and
the remote probe VLAN will not be deleted!
 Please wait... Done.
[Sysname] display vlan
The following VLANs exist:
  1(default), 7
```

The above output information indicates that VLAN 7 (the voice VLAN) cannot be removed, while the other VLANs are removed successfully.

Port-Based VLAN Configuration Commands

display port

Syntax

display port { **hybrid** | **trunk** }

View

Any view

Parameters

hybrid: Displays hybrid ports.

trunk: Displays trunk ports.

Description

Use the **display port** command to display the existing hybrid or trunk ports, if any.

For information about port type configuration, refer to the **port link-type** command.

Examples

Display the existing hybrid ports.

```
<Sysname> display port hybrid
The following hybrid ports exist:
  GigabitEthernet1/0/1          GigabitEthernet1/0/2
```

The above information shows the current system has two hybrid ports: GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

port

Syntax

port *interface-list*

undo port *interface-list*

View

VLAN view

Parameters

interface-list: List of the Ethernet ports to be added to or removed from the current VLAN. In this list, you can specify individual ports and port ranges. An individual port takes the form of *interface-type interface-number* and a port range takes the form of *interface-type interface-number1* **to** *interface-type interface-number2*, with *interface-number2* taking a value no less than *interface-number1*. The total number of individual ports and port ranges defined in the list must not exceed 10.

Description

Use the **port** command to assign one or multiple access ports to the current VLAN.

Use the **undo port** command to remove the specified access port(s) from the current VLAN.

The command applies to access ports only. For information about how to assign to or remove from a VLAN trunk or hybrid ports, refer to the **port hybrid vlan** command and the **port trunk permit vlan** command. For port type configuration, refer to the **port link-type** command.

Related commands: **display vlan**.

Examples

Assign GigabitEthernet1/0/2 through GigabitEthernet1/0/4 to VLAN 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/2 to GigabitEthernet 1/0/4
```

port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

View

Ethernet port view

Parameters

vlan-id: Specifies the ID of the VLAN to which you want to assign the current port, in the range of 1 to 4094. The specified VLAN must already exist.

Caution

By default, all access ports belong to VLAN 1. You cannot assign an access port to or remove an access port from VLAN 1 with the **port access vlan** command or its **undo** form. To assign an access port that has been assigned to a VLAN other than VLAN 1, you can use the **undo port access vlan** command.

Description

Use the **port access vlan** command to assign the current access port to the specified VLAN.

Use the **undo port access vlan** command to remove the access port from the specified VLAN. After that, the access port joins VLAN 1 automatically.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

port hybrid pvid vlan

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

View

Ethernet port view

Parameters

vlan-id: Specifies the default VLAN ID of the current hybrid port, in the range of 1 to 4094. The specified VLAN can be one already created or not.

Description

Use the **port hybrid pvid vlan** command to set the default VLAN ID of the hybrid port.

Use the **undo port hybrid pvid** command to restore the default VLAN ID of the hybrid port.

If the specified default VLAN has been removed or is not carried on the hybrid port, the port will be unable to receive VLAN untagged packets. You can configure a hybrid port to permit the packets of its default VLAN to pass through with the **port hybrid vlan** command.

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

Caution

The local and remote hybrid ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

Examples

Set the default VLAN ID of the hybrid port GigabitEthernet 1/0/1 to 100.

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

```
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
```

port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View

Ethernet port view

Parameters

vlan-id-list: List of the VLANs that the current hybrid port will be assigned to or removed from. In this list, you can specify individual VLAN IDs (each in the form of *vlan-id*) and VLAN ID ranges (each in the form of *vlan-id1* **to** *vlan-id2*). Specify each VLAN ID in the range of 1 to 4094 and ensure that *vlan-id2* is no less than *vlan-id1*. The total number of individual VLAN IDs and VLAN ID ranges defined in the list must not exceed 10. Be sure that the specified VLANs already exist.

tagged: Keeps VLAN tags when the packets of the specified VLANs are forwarded on the port.

untagged: Removes VLAN tags when the packets of the specified VLANs are forwarded on the port.

Description

Use the **port hybrid vlan** command to assign the hybrid port to one or multiple VLANs and configure the port to send packets tagged or untagged for the VLAN(s).

Use the **undo port hybrid vlan** command to remove the hybrid port from the specified VLAN(s).

By default, a hybrid port only allows packets from VLAN 1 to pass through untagged.

You can configure the **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } command multiple times. The VLANs specified each time does not overwrite those configured before, if any.

The VLAN specified by the *vlan-id* argument must already exist. Otherwise, this command is invalid.

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

Examples

Assign hybrid port GigabitEthernet 1/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100; configure the port to keep VLAN tags when sending the packets of these VLANs.

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

port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

View

Ethernet port view

Parameters

access: Sets the link type of the current port to access.

hybrid: Sets the link type of the current port to hybrid.

trunk: Sets the link type of the current port to trunk.

Description

Use the **port link-type** command to set the link type of the Ethernet port.

Use the **undo port link-type** command to restore the default link type.

The default link type of an Ethernet port is access.

 **Note**

To change the link type of a port from hybrid to trunk or vice versa, you need to change the link type to access first.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View

Ethernet port view

Parameters

vlan-id-list: List of the VLANs that the current trunk port will be assigned to or removed from. In this list, you can specify individual VLAN IDs (each in the form of *vlan-id*) and VLAN ID ranges (each in the form of *vlan-id1* **to** *vlan-id2*). Specify each VLAN ID in the range of 1 to 4094 and ensure that *vlan-id2* is no less than *vlan-id1*. The total number of individual VLAN IDs and VLAN ID ranges defined in the list must not exceed 10.

all: Assigns the trunk port to all VLANs. On a GVRP-enabled trunk port, you must configure the **port trunk permit vlan all** command to ensure that the traffic of all dynamically registered VLANs can pass through. However, When GVRP is disabled, you are discouraged to configure the keyword. This is to prevent users of unauthorized VLANs from accessing restricted resources through the port.

Description

Use the **port trunk permit vlan** command to assign the trunk port to the specified VLAN(s), that is, to allow packets from these VLANs to pass through the port.

Use the **undo port trunk permit vlan** command to remove the hybrid port from the specified VLAN(s).

By default, a trunk port belongs to VLAN 1 only.

On a trunk port, only traffic of the default VLAN can pass through untagged.

You can perform the command multiple times. The VLANs specified each time does not overwrite those configured before, if any.

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
System View: return to User View with Ctrl+Z.
[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.
```

port trunk pvid vlan

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

View

Ethernet port view

Parameters

vlan-id: Specifies the default VLAN ID of the current port, in the range of 1 to 4094.

Description

Use the **port trunk pvid vlan** command to set the default VLAN ID for the trunk port. A trunk port sends packets of the default VLAN untagged.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN ID of a trunk port is VLAN 1.

After configuring the default VLAN of a trunk port, you need to use the **port trunk permit vlan** command to configure the trunk port to allow the packets of the default VLAN to pass through.

If the specified default VLAN has been removed or is not carried on the trunk port, the port will be unable to receive VLAN untagged packets.

Note

The local and remote trunk ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

Related commands: **port link-type**, **port trunk permit vlan**.

Examples

Set the default VLAN ID of the trunk port GigabitEthernet 1/0/1 to 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Protocol-Based VLAN Configuration Commands

display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View

Any view

Parameters

interface-type interface-number: Specify a port by its type and number to display the protocol VLAN(s) bound with the port. You can use the *interface-type interface-number* **to** *interface-type interface-number* keyword and argument combination to specify a port range to display the protocol template information of the ports bound with protocol VLAN(s) in the range. When defining a port range, note that the second port must not be less than the first port.

all: Displays all the ports bound with at least one protocol VLAN and the associated protocol templates.

Description

Use the **display protocol-vlan interface** command to display information about protocol-based VLANs and protocol templates for the specified port(s).

Related commands: **port hybrid protocol-vlan vlan**, **protocol-vlan**.

Examples

Display the protocol VLAN information of ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<Sysname> display protocol-vlan interface GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2
 Interface: GigabitEthernet1/0/1
```

```
    VLAN ID   Protocol-Index     Protocol-type
       50          0                ip
       80          1                ip
       100         0                ip
       100         1                ipx ethernetii
Interface: GigabitEthernet1/0/2
    VLAN ID   Protocol-Index     Protocol-type
       50          1                ipx raw
       80          2                at
       100         3                snap etype 0x0abc
       100         4                llc dsap 0xac ssap 0xbd
```

Table 1-3 Description on the fields of the **display vlan** command

Field	Description
Interface	Interface bound with at least one protocol VLAN
VLAN ID	ID of a protocol VLAN bound with the interface
Protocol-Index	Protocol template index
Protocol-type	Protocol type specified by the protocol template. Refer to the **protocol-vlan** command for detailed description.

display protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

Any view

Parameters

vlan-id1: Specifies a VLAN ID in the range of 1 to 4094, of which the protocol VLAN configuration information is to be displayed.

to *vlan-id2*: In conjunction with *vlan-id1*, define a VLAN range to display the protocol template configurations of all protocol VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.

all: Displays all protocol VLANs and their protocol template information.

Description

Use the **display protocol-vlan vlan** command to display information about protocol VLANs.

Related commands: **protocol-vlan**.

Examples

Display the protocol information and protocol indexes configured for VLAN 10 through VLAN 20.

```
<Sysname> display protocol-vlan vlan 10 to 20
 VLAN ID: 10
```

```
VLAN Type: Protocol-based VLAN
     Protocol-Index          Protocol-Type
            0                    ip
            1                    ip
            2                    ipx ethernetii
            3                    at
VLAN ID: 15
VLAN Type: Protocol-based VLAN
     Protocol-Index          Protocol-Type
            0                    ip
            1                    snap etype 0x0abcd
```

Table 1-4 Description on the fields of the **display protocol-vlan vlan** command

Field	Description
VLAN ID	Protocol VLAN ID
VLAN Type	VLAN type. Here, it refers to Protocol-based VLAN
Protocol-Index	Protocol template index
Protocol-Type	Protocol type specified in the protocol template. Refer to the **protocol-vlan** command for detailed description.

port hybrid protocol-vlan vlan

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-index-end*] | **all** }

undo port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-index-end*] | **all** }

View

Ethernet port view

Parameters

vlan-id: Specifies the ID of the protocol VLAN bound with the port. The value range is 1 to 4094. At least one protocol template must have been configured for the VLAN.

protocol-index: Specifies a protocol template, in the range of 0 to 7.

to *protocol-index-end*: In conjunction with *protocol-index*, specify a protocol index range. The *protocol-index-end* argument takes a value in the range of 0 to 7 and must be greater than *protocol-index*.

all: Specifies all protocol indexes. With the **all** keyword, the **port hybrid protocol-vlan vlan** command binds the port with all the protocol templates of the specified protocol VLAN, and the **undo** form of the command removes the associations between the port and all the protocol templates of the specified protocol VLAN.

Description

Use the **port hybrid protocol-vlan vlan** command to bind the port with the specified protocol template(s) of a protocol VLAN.

Use the **undo port hybrid protocol-vlan vlan** command to remove the binding between the port and the specified protocol template(s) of a protocol VLAN.

Note

- The **port hybrid protocol-vlan vlan** command is available on hybrid ports only.
- Before you bind a port with a protocol VLAN, assign the port to the VLAN with the **port hybrid vlan** command. Otherwise, the binding will fail.
- To bind a protocol template to a port in a VLAN successfully, you must ensure that the protocol template has been created in the VLAN. If the protocol template you are binding with the port has not been created in the VLAN, the system will display the operation failure message. If some of the protocol templates you are binding with the port have not been created in the VLAN, the system does not display error messages while binding those already created with the port.
- When you removes the binding between a port and a protocol template, the system will report operation failure if the index of the specified protocol to be removed does not exist. If a part of the specified protocol indexes to be removed do not exist, the switch will remove the existing indexes when it prompts errors.

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

Examples

Bind GigabitEthernet 1/0/1 with the protocols indexed from 0 to 2 of VLAN 3 (assuming that VLAN 3 is a protocol VLAN).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 3 0 to 2
```

Remove the binding between GigabitEthernet 1/0/1 and protocols indexed from 1 to 4 of VLAN 3.

```
[Sysname-GigabitEthernet1/0/1] undo port hybrid protocol-vlan vlan 3 1 to 4
 Protocol index 1 does not exist in VLAN 3
 Protocol index 4 does not exist in VLAN 3
```

protocol-vlan

Syntax

protocol-vlan [*protocol-index*] { **at** | **ip** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc dsap** *dsap-id* **ssap** *ssap-id* | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-index-end*] | **all** }

View

VLAN view

Parameters

at: Creates the AppleTalk-based protocol template.

ip: Creates the IP-based protocol template.

ipx: Creates the IPX-based protocol template. The **ethernetii**, **llc**, **raw** and **snap** keywords represent four IPX encapsulation formats. For more information about encapsulation formats, refer to the accompanying operation manual.

mode: Configures a user-defined protocol template.

ethernetii *etype-id*: Creates the protocol template that matches the Ethernet II encapsulation format and the corresponding protocol type value of the packet. The *etype-id* argument indicates the protocol type value and ranges from 0x0600 to 0xFFFF(excluding 0x0800, 0x8137, and 0x809b).

llc: Creates the protocol template that matches LLC encapsulation format.

dsap-id: Destination service access point. This argument ranges 0x00 to 0xFF.

ssap-id: Source service access point. This argument ranges from 0x00 to 0xFF.

snap *etype-id*: Creates a protocol template that matches SNAP encapsulation format and the corresponding protocol type value of the packet. The *etype-id* argument indicates the protocol type value and ranges from 0x0600 to 0xFFFF.

protocol-index: Beginning protocol index ranging from 0 to 7. If you do not specify this argument, the beginning protocol index will be determined by the system.

protocol-index-end: End protocol index ranging from 0 to 7. Note that this argument must be larger than or equal to the *protocol-index* argument.

all: Deletes all the protocol templates.

Note

When you use the **mode** keyword to configure a user-defined protocol template, if you set the *etype-id* argument for Ethernet II or SNAP packets to 0x0800, 0x8137, or 0x809B, the matching packets will have the same format as that of IP, IPX, and AppleTalk packets respectively. To prevent two commands from processing packets of the same matching conditions in different ways, the switch will prompt that you cannot set the *etype-id* argument for Ethernet II or SNAP packets to 0x0800, 0x8137, or 0x809B.

Description

Use the **protocol-vlan** command to configure the protocol template used for classifying protocol-based VLANs.

Use the **undo protocol-vlan** command to disable the configuration.

By default, no protocol template is configured.

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

Examples

Configure VLAN 3 as a protocol-based VLAN and assign IP packets to VLAN 3 for transmission.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan ip
```

Caution

Because the IP protocol is closely associated with the ARP protocol, you are recommended to configure the ARP protocol type when configuring the IP protocol type and associate the two protocol types with the same port, in case that ARP packets and IP packets are not assigned to the same VLAN, which will cause IP address resolution failure.

Configure an ARP protocol template. The code for the ARP protocol is 0x0806.

- Perform the following command when Ethernet encapsulation is used.

```
[Sysname-vlan3] protocol-vlan mode ethernetii etype 0806
```

- Perform the following configuration when 802.3 encapsulation format is used.

```
[Sysname-vlan3] protocol-vlan mode snap etype 0806
```

Table of Contents

1 Static Routing Configuration Commands

Static Routing Configuration Commands

delete static-routes all

Syntax

delete static-routes all

View

System view

Parameter

None

Description

Use the **delete static-routes all** command to delete all static routes.

The system will request your confirmation before it deletes all the configured static routes.

Related command: **ip route-static** and **display ip routing-table**.

Example

Delete all the static routes in the router.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] delete static-routes all
Are you sure to delete all the unicast static routes?[Y/N]y
```

display ip routing-table

Syntax

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

View

Any view

Parameter

regular-expression: Regular expression, which specifies a match character string.

|: Uses the regular expression to match the output routing information.

begin: Displays the routing information from the route entry containing the specified character string.

include: Displays all routing information containing the specified character string.

exclude: Displays all routing information without the specified character string.

Description

Use the **display ip routing-table** command to display the summary information about the routing table.

This command displays the summary information about a routing table, with the items of a routing entry contained in one line. The information displayed includes destination IP address/mask length, protocol, preference, cost, next hop and outbound interface.

The **display ip routing-table** command only displays the routes currently in use, that is, the optimal routes.

Example

Display the summary information about the routing table.

```
<Sysname> display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
127.0.0.0/8         DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.1/32        DIRECT   0    0           127.0.0.1       InLoopBack0
```

Table 1-1 Description on the fields of the **display ip routing-table** command

Field	Description
Destination/Mask	Destination IP address/mask length
Protocol	Routing protocol that discovers the route
Pre	Route preference
Cost	Route cost
Nexthop	Next hop IP address of the route
Interface	Outbound interface, through which packets destined for the destination network segment are to be transmitted

display ip routing-table acl

Syntax

display ip routing-table acl *acl-number* [**verbose**]

View

Any view

Parameter

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

verbose: Displays the detailed information about the active and inactive routes that match the specified ACL. If you do not specify this keyword, only the summary information about the active routes matching the specified ACL is displayed.

Description

Use the **display ip routing-table acl** command to display the routes that match a specified basic ACL.

As this command displays the routes that match a specified basic ACL, you can use it to trace routing policies.

Example

Display the summary information about the active routes that match ACL 2000.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[Sysname-acl-basic-2000] rule deny source any
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes matched by access-list 2000:
  Summary count: 1
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
10.1.1.0/24         STATIC   60   0           192.168.0.31    Vlan-interface1
```

Refer to Table 1-1 for the description on the output fields.

Display the detailed information about the active and inactive routes that match ACL 2000.

```
[Sysname] display ip routing-table acl 2000 verbose
Routes matched by access-list 2000:
  + = Active Route, - = Last Active, # = Both    * = Next hop in use

  Summary count: 1

**Destination: 10.1.1.0          Mask: 255.255.255.0
         Protocol: #STATIC       Preference: 60
         *NextHop: 192.168.0.31     Interface: 192.168.0.51(Vlan-interface1)
         State: <Int ActiveU Gateway Static Unicast>
         Age: 1:48:18            Cost: 0/0
```

Table 1-2 Description on the fields of the **display ip routing-table acl** command

Field	Description
Destination	Destination address
Mask	Mask
Protocol	Routing protocol that discovers the route
Preference	Route preference
Nexthop	Next hop IP address
Interface	Outbound interface, through which packets destined for the destination network segment are to be transmitted

Field	Description	
State	Descriptions on the route state are as follows:	
	ActiveU	Valid unicast route. “U” stands for unicast.
	Blackhole	Blackhole route is the same as reject route except that a router drops a packet traveling along a blackhole route without sending ICMP unreachable messages to the source of the packets.
	Delete	The route is deleted.
	Gateway	The route is not a direct route.
	Hidden	The route is a hidden route. The system hides routes that are temporarily unavailable for some reasons (such as the policy configured or the interface is down) for later use.
	Holddown	The route is held down. Holddown is a kind of route advertisement policy used in some D-V (distance vector) routing protocols (such as RIP) to avoid the propagation of some incorrect routes and improve the transmission speed of route-unreachable information. For details, refer to corresponding routing protocols.
	Int	The route is discovered by the internal gateway protocol (IGP).
	NoAdvise	The route is not advertised when the router advertises routes based on policies
	NotInstall	The route are not loaded to the core routing table but can be advertised. Normally, the routes with the highest preference in the routing table are loaded to the core routing table and are advertised.
	Reject	The packets travel along the route will be dropped. Besides, the router sends ICMP unreachable messages to the source of the dropped packets. The Reject routes are usually used for network testing.
	Retain	The route is not deleted when the routes in the core routing table are deleted. You can enable static routes to remain in the core routing table by configure them to be in retain state.
	Static	Static routes configured manually on the router are marked as static. Such routes are not lost when you perform the save operation and then restart the router.
	Unicast	The route is a unicast route.
Age	Time period during which the route is allowed to be in the routing table, in the form of hh:mm:ss.	
Cost	Cost of the route	

display ip routing-table *ip-address*

Syntax

display ip routing-table *ip-address* [*mask*] [**longer-match**] [**verbose**]

View

Any view

Parameter

ip-address: Destination IP address, in dotted decimal notation.

mask: Mask of the destination IP address, which can be in dotted decimal notation or be an integer ranging from 0 to 32.

longer-match: Displays all the routes leading to the destination coupled with the default mask.

verbose: Displays the detailed information about the active and inactive routes leading to the destination. If this keyword is not specified, only the summary information about the active routes is displayed.

Description

Use the **display ip routing-table** *ip-address* command to display the information about the routes leading to a specified destination.

The output information of this command differs with the arguments/keywords specified as follows:

- **display ip routing-table** *ip-address*

For the destination address *ip-address*, if there are some routes matched within the natural mask range, the active routes which best match *ip-address* are displayed.

- **display ip routing-table** *ip-address mask*

Only the routes which match exactly the specified destination address and mask are displayed.

- **display ip routing-table** *ip-address* **longer-match**

All routes with their destination addresses matched within the natural mask range are displayed.

- **display ip routing-table** *ip-address mask* **longer-match**

All routes with their destination addresses matched within the specified mask range are displayed.

Example

Display the summary information of the routes with their destination addresses matched within the natural mask range.

```
<Sysname> display ip routing-table 169.0.0.0
Destination/Mask       Protocol Pre Cost     Nexthop      Interface
169.0.0.0/16           Static   60  0        2.1.1.1      LoopBack1
```

Refer to Table 1-1 for the description on the output fields.

Display the detailed information of the routes with their destination addresses matched within the natural mask range.

```
<Sysname> display ip routing-table 169.0.0.0 verbose
Routing tables:
  + = Active Route, - = Last Active, # = Both    * = Next hop in use
  Summary count: 1
**Destination: 169.0.0.0         Mask: 255.255.255.0
         Protocol: #STATIC       Preference: 60
         *NextHop: 2.1.1.1          Interface: 2.1.1.1(LoopBack1)
         State: <Int ActiveU Gateway Static Unicast>
         Age: 4:49               Cost: 0/0
```

Refer to Table 1-2 for the description on the output fields.

display ip routing-table *ip-address1 ip-address2*

Syntax

display ip routing-table *ip-address1 mask1 ip-address2 mask2* [**verbose**]

View

Any view

Parameter

ip-address1, *ip-address2*: Destination IP addresses in dotted decimal notation. *ip-address1* and *mask1*, together with *ip-address2* and *mask2*, determine an IP address range. The starting address of the IP address range is determined by the *ip-address1* and *mask1* arguments; and the end address of the IP address range is determined by the *ip-address2* and *mask2* arguments.

mask1, *mask2*: IP address masks. These two arguments can be in dotted decimal notation or two integers ranging from 0 to 32.

verbose: Displays the detailed information about the active and inactive routes. If you do not specify this keyword, only the summary information about the active routes is displayed.

Description

Use the **display ip routing-table** *ip-address1 ip-address2* command to display the information about the routes with their destinations within the specified destination IP address range.

Example

Display the information about the routes with their destinations within the range of 1.1.1.0 to 2.2.2.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 2.2.2.0 24
Routing tables:
  Summary count: 1
Destination/Mask   Protocol   Pre Cost        Nexthop      Interface
1.1.1.0/24          DIRECT     0   0          1.1.1.1      Vlan-interface1
```

Refer to Table 1-1 for the description on the output fields.

display ip routing-table ip-prefix

Syntax

display ip routing-table ip-prefix *ip-prefix-name* [**verbose**]

View

Any view

Parameter

ip-prefix-name: Name of an IP prefix list, a string comprising 1 to 19 characters.

verbose: Displays the detailed information about the active and inactive routes matching a specified IP prefix list. If you do not specify this keyword, only the summary information about the active routes matching the IP prefix list is displayed.

Description

Use the **display ip routing-table ip-prefix** command to display the information about the routes matching a specified IP prefix list.

You can use this command to trace routing policies and display the routes matching a specified IP prefix list.

If the specified IP prefix list does not exist, the detailed information about all the active and inactive routes is displayed when you execute this command with the **verbose** keyword specified, and only the summary information about all the active routes is displayed if you execute this command with the **verbose** keyword not specified.

Example

Display the summary information about the active routes matching the IP prefix list named abc2.

```
<Sysname> display ip routing-table ip-prefix abc2
Routes matched by ip-prefix abc2:
  Summary count: 2
Destination/Mask    Protocol Pre  Cost       Nexthop         Interface
10.1.1.0/24         DIRECT   0    0           10.1.1.2        Vlan-interface1
10.1.1.2/32         DIRECT   0    0          127.0.0.1        InLoopBack0
```

Refer to Table 1-1 for the description on the output fields.

Display the detailed information about the active and inactive routes matching the IP prefix list named abc2.

```
<Sysname> display ip routing-table ip-prefix abc2 verbose
Routes matched by ip-prefix abc2:
  + = Active Route, - = Last Active, # = Both   * = Next hop in use

  Summary count: 2

**Destination: 10.1.1.0         Mask: 255.255.255.0
        Protocol: #DIRECT       Preference: 0
        *NextHop: 10.1.1.2         Interface: 10.1.1.2(Vlan-interface1)
        State: <Int ActiveU Retain Unicast>
        Age: 3:23:44            Cost: 0/0

**Destination: 10.1.1.2         Mask: 255.255.255.255
        Protocol: #DIRECT       Preference: 0
        *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
        State: <NoAdvise Int ActiveU Retain Gateway Unicast>
        Age: 3:23:44            Cost: 0/0
```

Refer to Table 1-2 for the description on the output fields.

display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

View

Any view

Parameter

protocol: This argument can be one of the following:

- **direct**: Displays the information about the direct routes.
- **static**: Displays the information about the static routes.

inactive: Displays the information about the inactive routes. If you do not specify this keyword, the information about both active and inactive routes is displayed.

verbose: Displays the detailed route information. If you do not specify this keyword, only the summary route information is displayed.

Description

Use the **display ip routing-table protocol** command to display the information about specified type of routes.

Example

Display the summary information about all the direct routes.

```
<Sysname> display ip routing-table protocol direct
DIRECT Routing tables:
Summary count: 4
DIRECT Routing tables status:<active>:
Summary count: 3
Destination/Mask       Protocol    Pre Cost     Nexthop      Interface
20.1.1.1/32            DIRECT      0   0        127.0.0.1    InLoopBack0
127.0.0.0/8            DIRECT      0   0        127.0.0.1    InLoopBack0
127.0.0.1/32           DIRECT      0   0        127.0.0.1    InLoopBack0
DIRECT Routing tables status:<inactive>:
Summary count: 1
Destination/Mask       Protocol   Pre   Cost     Nexthop      Interface
210.0.0.1/32           DIRECT      0    0        127.0.0.1    InLoopBack0
```

Display the summary information about the static routing table.

```
<Sysname> display ip routing-table protocol static
STATIC Routing tables:
  Summary count: 1
STATIC Routing tables status:<active>:
  Summary count: 0
STATIC Routing tables status:<inactive>:
  Summary count: 1
Destination/Mask   Protocol   Pre Cost       Nexthop      Interface
1.2.3.0/24          STATIC     60  0         1.2.4.5      Vlan-interface1
```

Refer to Table 1-1 for the description on the output fields.

display ip routing-table radix

Syntax

display ip routing-table radix

View

Any view

Parameter

None

Description

Use the **display ip routing-table radix** command to display the information about the routes in a routing table in a hierarchical way.

Example

Display the information about the routes in a routing table in a hierarchical way.

```
<Sysname> display ip routing-table radix
Radix tree for INET (2) inodes 2 routes 2:

                    +--8+--{127.0.0.0
                       +-32+--{127.0.0.1
```

Table 1-3 Description on the fields of the **display ip routing-table radix** command

Field	Description
INET	Address family
inodes	Number of nodes
routes	Number of routes

display ip routing-table statistics

Syntax

display ip routing-table statistics

View

Any view

Parameter

None

Description

Use the **display ip routing-table statistics** command to display the statistics of a routing table.

The statistics information displayed by this command includes:

- The total number of the routes

- The number of the active routes
- The number of the added routes
- The number of the routes with deleted flags

Example

Display the statistics information about the routing table.

```
<Sysname> display ip routing-table statistics
Routing tables:
Proto      route       active      added       deleted
DIRECT     2            2           2           0
STATIC     0            0           0           0
Total      2            2           2           0
```

Table 1-4 Description on the fields of the **display ip routing-table statistics** command

Field	Description
Proto	Routing protocol
route	Total number of routes
active	Number of the active routes that are currently in use
added	Number of the routes that are added to the routing table after the switch starts or the routing table is cleared last time
deleted	Number of the routes with deleted flags (this type of routes will be removed after a period of time)
Total	Total numbers of various routes

display ip routing-table verbose

Syntax

display ip routing-table verbose

View

Any view

Parameter

None

Description

Use the **display ip routing-table verbose** command to display the detailed information about a routing table.

You can use this command to display all the routes, including the inactive and invalid routes.

Example

Display the detailed information about the routing table.

```
<Sysname> display ip routing-table verbose
Routing Tables:
```

```
  + = Active Route, - = Last Active, # = Both   * = Next hop in use

  Destinations: 2       Routes: 2
  Holddown: 0   Delete: 0       Hidden: 0

**Destination: 127.0.0.0        Mask: 255.0.0.0
        Protocol: #DIRECT       Preference: 0
        *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
        State: <NoAdvise Int ActiveU Retain Unicast>
        Age: 57:12      Cost: 0/0

**Destination: 127.0.0.1        Mask: 255.255.255.255
        Protocol: #DIRECT       Preference: 0
        *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
        State: <NotInstall NoAdvise Int ActiveU Retain Gateway Unicast>
        Age: 57:12      Cost: 0/0
```

The statistics of the routing table are displayed first, and then the detailed descriptions of each route. Table 1-2 describes the route states and Table 1-5 describes the statistics information about the routing table.

Table 1-5 Description on the fields of the **display ip routing-table verbose** command

Field	Description
Holddown	Number of the routes that are held down
Delete	Number of the deleted routes
Hidden	Number of the hidden routes

ip route-static

Syntax

ip route-static *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**description** *text*]

undo ip route-static *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | *next-hop*] [**preference** *preference-value*]

View

System view

Parameter

ip-address: Destination IP address, in dotted decimal notation.

mask: IP address mask, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

interface-type interface-number: Next hop outgoing interface. A null interface is a virtual interface. Packets destined for a null interface are discarded, helping to reduce system load.

next-hop: IP address of the next hop of this route, in dotted decimal notation.

preference-value: Preference of this route, in the range of 1 to 255.

reject: Specifies the route as an unreachable route. When a static route destined for a destination address is of the **reject** attribute, all the IP packets destined for the destination address are discarded, and the source host is informed that the destination address is unreachable.

blackhole: Specifies the route as a black hole route. When a static route destined for a destination address is of the **blackhole** attribute, the outgoing interface of the route is Null 0 regardless of the next hop address. All the IP packets destined for the destination address are discarded, and the source host is not informed that the destination address is unreachable.

description *text*: Specifies a descriptive string for the static route. The *text* argument is a case-sensitive string of 1 to 60 characters (including the space).

Description

Use the **ip route-static** command to configure a static route.

Use the **undo ip route-static** command to remove a static route.

By default, the system can obtain the subnet route directly connected to the router. When you configure a static route, if no preference is specified for the route, the preference defaults to 60. Note that routes with the same destinations, the same next hops, but different preferences are different routes. Among these routes, the one with least preference (which means the highest preference) is chosen to be the current route. A route configured using the **ip route-static** command is a reachable route if neither of the **reject** and **blackhole** keywords is specified.

Note the following when configuring a static route:

- The next hop address of a static route cannot be the VLAN interface address of the local switch.
- A static route with both its destination IP address and mask both being 0.0.0.0 is the default route. When no matched entry is found in the routing table, a received packet is forwarded according to the default route.

Related command: **display ip routing-table**.

Example

Configure the next hop of the default route as 129.102.0.2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { **all** | *protocol* }

View

User view

Parameter

all: Specifies all protocols.

protocol: Specifies a protocol, which can be **static**, or **direct**.

Description

Use the **reset ip routing-table statistics protocol** command to clear the statistics of routes in a routing table.

Example

Before executing the **reset ip routing-table statistics protocol** command, use the **display ip routing-table statistics** command to display the routing statistics:

```
<Sysname> display ip routing-table statistics
Routing tables:
Proto      route       active      added       deleted
DIRECT     4           4           24          20
STATIC     0           0           1           1
Total      4           4           25          21
```

Clear the routing statistics of all protocols from the IP routing table.

```
<Sysname> reset ip routing-table statistics protocol all
This will erase the specific routing counters information.
Are you sure?[Y/N]y
```

Display the routing statistics in the IP routing table.

```
<Sysname> display ip routing-table statistics
Routing tables:
Proto      route       active      added       deleted
DIRECT     4           4           0           0
STATIC     0           0           0           0
Total      4           4           0           0
```

The above information shows that the routing statistics in the IP routing table is cleared.

Table of Contents

1 Voice VLAN Configuration Commands

Voice VLAN Configuration Commands

display voice vlan error-info

Syntax

display voice vlan error-info

View

Any view

Parameters

None

Description

Use the **display voice vlan error-info** command to display the ports on which the voice VLAN function fails to be enabled.

Note

When ACL number applied to a port reaches to its threshold, voice VLAN cannot be enabled on this port.

Examples

Display the ports on which voice VLAN fails to be enabled.

```
<Sysname> display voice vlan error-info
Fail to apply voice VLAN ACL rules to the following port(s):
  GigabitEthernet1/0/10    GigabitEthernet1/0/15
```

display voice vlan oui

Syntax

display voice vlan oui

View

Any view

Parameters

None

Description

Use the **display voice vlan oui** command to display the organizationally unique identifier (OUI) list used for identifying voice traffic.

The output of the command displays the OUI addresses, their masks, and descriptions.

By default, there are five pre-defined OUI addresses in the system. You can use the **voice vlan mac-address** command to add, modify, or remove OUI addresses.

Examples

Display the OUI list for the voice VLAN.

```
<Sysname> display voice vlan oui
Oui Address      Mask           Description
0003-6b00-0000  ffff-ff00-0000  Cisco phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

display voice vlan status

Syntax

display voice vlan status

View

Any view

Parameters

None

Description

Use the **display voice vlan status** command to display voice VLAN-related information.

The output of the command displays information such as the voice VLAN security mode and voice VLAN assignment mode (manual or automatic).

Related commands: **voice vlan**, **voice vlan enable**.

Examples

Display the information about the voice VLAN.

```
<Sysname> display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
```

```
PORT                      MODE     COS  DSCP
-------------------------------------------
GigabitEthernet1/0/1      AUTO     5    40
GigabitEthernet1/0/2      MANUAL   4    40
```

Table 1-1 Description on the fields of the **display voice vlan status** command

Field	Description
Voice Vlan status	The status of global voice VLAN function: enabled or disabled.
Voice Vlan ID	The VLAN which is currently enabled with voice VLAN.
Voice Vlan security mode	The status of voice VLAN security mode: enabled or disabled.
Voice Vlan aging time	The voice VLAN aging time
Current voice vlan enable port mode	The ports on which the voice VLAN function is enabled.
PORT	Port number
MODE	Voice VLAN assignment mode on the port, which can be auto or manual.
COS	The CoS precedence marked on the voice traffic passing through the port.
DSCP	The DSCP precedence marked on the voice traffic passing through the port.

Caution

The **Current voice vlan enable port mode** field lists the ports with the voice VLAN function enabled. Note that not all of them are transmitting packets in the voice VLAN. To view the ports operating in the voice VLAN currently, use the **display vlan** command.

display vlan

Syntax

display vlan *vlan-id*

View

Any view

Parameters

vlan-id: Specifies the ID of the current voice VLAN in the range of 1 to 4094.

Description

Use the **display vlan** command to display information about the specified VLAN.

For the voice VLAN, this command displays all the ports in the VLAN.

Related commands: **voice vlan**, **voice vlan enable**.

Examples

Display all the ports in the current voice VLAN, assuming that the current voice VLAN is VLAN 6.

```
<Sysname> display vlan 6
 VLAN ID: 6
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0006
 Name: VLAN 0006
 Tagged   Ports:
  GigabitEthernet1/0/5
 Untagged Ports:
  GigabitEthernet1/0/6
```

The output indicates that GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 are in the voice VLAN.

voice vlan

Syntax

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

undo voice vlan enable

View

System view

Parameters

vlan-id: Specifies the ID of the VLAN to be enabled with the voice VLAN function, in the range of 2 to 4094. Note that the VLAN must already exist.

Description

Use the **voice vlan** command to configure the specified VLAN as the voice VLAN, that is, enable voice VLAN globally.

Use the **undo voice vlan enable** command to remove the voice VLAN configuration from the specified VLAN.

By default, voice VLAN is disabled globally.

After a VLAN is configured as the voice VLAN, the switch will modify QoS priorities for the traffic in the VLAN to improve its transmission preference, guaranteeing that the voice data can be transmitted preferentially.

To make the voice VLAN function take effect on a port, you must enable the function both globally and on the port with the **voice vlan enable** command.

Caution

- If you want to delete a VLAN with voice VLAN function enabled, you must disable the voice VLAN function first.
- The voice VLAN function can be enabled for only one VLAN at one time.

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

Examples

Create VLAN 2, and enable the voice VLAN function on it.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] voice vlan 2 enable
```

After the voice VLAN function of VLAN 2 is enabled, if you enable the voice VLAN function for other VLANs, the system will prompt that your configuration fails.

```
[Sysname] voice vlan 4 enable
Can't change voice vlan configuration when other voice vlan is running
```

voice vlan aging

Syntax

voice vlan aging *minutes*

undo voice vlan aging

View

System view

Parameters

minutes: Sets the voice VLAN aging timer in minutes, in the range of 5 to 43200.

Description

Use the **voice vlan aging** command to set the voice VLAN aging timer.

Use the **undo voice vlan aging** command to restore the default.

By default, the voice VLAN aging timer is 1440 minutes.

If a port is configured to work in automatic voice VLAN assignment mode, the switch automatically assigns the port to the voice VLAN when receiving a packet with the source MAC address matching an entry in the OUI list of the switch. As soon as the port is assigned to the voice VLAN, the voice VLAN aging timer starts. If no recognizable voice traffic has been received before the timer expires, the port is removed from the voice VLAN.

The voice VLAN aging timer does not take effect on ports working in manual voice VLAN assignment mode, because these ports are assigned to the voice VLAN statically.

When setting the voice VLAN aging timer, consider the usage frequency of IP phones. Note that:

- A large voice VLAN aging timer setting can prevent a port from being assigned to or removed from the voice VLAN frequently, keeping voice communication stable. However, this may cause a port to stay in the voice VLAN even if it has not transmitted voice traffic for a long time, occupying system resources and bringing about security problems. Therefore, you are recommended to set a large voice VLAN aging timer in a network with credible network devices and many voice applications.
- A small voice VLAN aging timer enables the switch to remove a port that has not transmitted voice traffic from the voice VLAN timely, thus improving network security. However, this may cause the port to be assigned to or removed from the voice VLAN frequently. Therefore, you are recommended to set a small voice VLAN aging timer in a network with only a few voice applications.

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

Examples

Set the aging time of the voice VLAN to 100 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] voice vlan aging 100
```

voice vlan enable

Syntax

voice vlan enable

undo voice vlan enable

View

Ethernet port view

Parameters

None

Description

Use the **voice vlan enable** command to enable the voice VLAN function on the port.

Use the **undo voice vlan enable** command to disable the voice VLAN function on the port.

By default, the voice VLAN function is disabled on all ports.

To have the voice VLAN function take effect on a port, you must enable it both globally and on the port. Note that the operations are order independent.

Related commands: **display voice vlan error-info**, **display voice vlan status**.

Examples

Enable the voice VLAN function on GigabitEthernet1/0/2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] voice vlan enable
```

voice vlan legacy

Syntax

voice vlan legacy

undo voice vlan legacy

View

Ethernet port view

Parameters

None

Description

Use the **voice vlan legacy** command to realize the communication between 3Com device and other vendors' voice device by automatically adding the voice VLAN tag to the voice data coming from other vendors' voice device.

Use the **undo voice vlan legacy** command to disable the voice VLAN legacy function.

By default, the voice VLAN legacy function is disabled.

Examples

Enable the voice VLAN legacy function on GigabitEthernet1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan legacy
```

voice vlan mac-address

Syntax

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

undo voice vlan mac-address *oui*

View

System view

Parameters

oui: Specify a MAC address, in the format of H-H-H.

oui-mask: Specify a MAC address mask, made up of consecutive Fs and consecutive 0s. It specifies the matching length of the OUI address. When the switch receives a packet, it matches the bits in the source MAC address corresponding to the Fs against the OUI list.

text: Description of the MAC address, containing 1 to 30 characters.

Description

Use the **voice vlan mac-address** command to add an OUI entry to the OUI list for the specified MAC address. The OUI list contains the MAC addresses of recognizable voice devices. A packet is considered as a voice packet only when its source MAC address can match an entry in the OUI list.

Use the **undo voice vlan mac-address** command to remove an OUI entry from the OUI list.

By default, the OUI list contains the five pre-defined OUI addresses in Table 1-2. You can modify them with the **voice vlan mac-address** command.

The OUI list can contain up to 16 OUI address entries.

Table 1-2 Default OUI addresses of a switch

Number	OUI address	Vendor
1	0003-6b00-0000	Cisco phone
2	000f-e200-0000	H3C Aolynk phone
3	00d0-1e00-0000	Pingtel phone
4	00e0-7500-0000	Polycom phone
5	00e0-bb00-0000	3Com phone

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

Examples

Add MAC address 00aa-bb00-0000 to the OUI list and configure its description as ABC.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] voice vlan mac-address 00aa-bb00-0000 mask ffff-ff00-0000 description ABC
```

voice vlan mode

Syntax

voice vlan mode auto

undo voice vlan mode auto

View

Ethernet port view

Parameters

None

Description

Use the **voice vlan mode auto** command to configure the voice VLAN assignment mode of the Ethernet port to automatic.

Use the **undo voice vlan mode auto** command to configure the voice VLAN assignment mode of the Ethernet port to manual.

You cannot and need not to assign a port working in automatic voice VLAN assignment mode to the voice VLAN manually. When the port receives a packet whose source MAC address matches the OUI list, the port is assigned to the voice VLAN automatically, and the packet is tagged with the voice VLAN tag. If the port has not received any voice data before the voice VLAN aging timer expires, the port is removed from the voice VLAN automatically.

By default, an Ethernet port works in automatic voice VLAN assignment mode.

A port working in manual voice VLAN assignment mode needs to be assigned to the voice VLAN manually. The port stays in the voice VLAN no matter whether voice data is present on the port, that is, the voice VLAN aging timer does not take effect on the port.

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

Examples

Configure the voice VLAN assignment mode on GigabitEthernet1/0/2 to manual.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] undo voice vlan mode auto
```

voice vlan qos

Syntax

voice vlan qos { *cos-value dscp-value* | **trust** }

undo voice vlan qos

View

Ethernet port view

Parameters

cos-value: Sets the CoS precedence marked for voice VLAN traffic, in the range 0 to 7.

dscp-value: Sets the DSCP precedence marked for voice VLAN traffic, in the range 0 to 63.

trust: Sets the port to trust the priorities of voice VLAN traffic passing through it, that is, the CoS precedence or the DSCP precedence carried in voice VLAN traffic.

Description

Use the **voice vlan qos** command to modify the CoS precedence and DSCP precedence to be marked for voice VLAN traffic.

Use the **undo voice vlan qos** command to restore the default.

By default, the CoS precedence and the DSCP precedence marked for voice VLAN traffic are 6 and 46.

After the CoS and DSCP precedence values marked for voice VLAN traffic are changed, the switch will use the changed precedence values to look for the matching local precedence when queuing voice VLAN traffic. For more information about local precedence and queuing, refer to the QoS-QoS Profile part of this manual.

Examples

Modify the CoS precedence and the DSCP precedence marked for voice VLAN traffic passing through GigabitEthernet 1/0/1 to 5 and 40 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan qos 5 40
```

voice vlan security enable

Syntax

voice vlan security enable

undo voice vlan security enable

View

System view

Parameters

None

Description

Use the **voice vlan security enable** command to enable the voice VLAN security mode.

Use the **undo voice vlan security enable** command to disable the voice VLAN security mode.

In security mode, the ports in a voice VLAN and with voice devices attached to can only forward voice data. Data packets with their MAC addresses not among the OUI addresses that can be identified by the system will be filtered out. This mode has no effects on other VLANs.

By default, the voice VLAN security mode is enabled.

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

Examples

Disable the voice VLAN security mode.

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

Table of Contents

1 GVRP Configuration Commands

GARP Configuration Commands

display garp statistics

Syntax

display garp statistics [**interface** *interface-list*]

View

Any view

Parameters

interface-list: Specifies a list of Ethernet ports for which the statistics about GARP are to be displayed. In this list, you can specify individual ports and port ranges. An individual port takes the form of *interface-type interface-number* and a port range takes the form of *interface-type interface-number1* **to** *interface-type interface-number2*, with *interface-number2* taking a value greater than *interface-number1*. The total number of individual ports and port ranges defined in the list must not exceed 10.

Description

Use the **display garp statistics** command to display the GARP statistics of the specified or all ports. If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP statistics on all the ports.

The switch automatically collects statistics about GVRP packets sent, received and dropped on GVRP-enabled ports. Upon system reboot or the execution of the **reset garp statistics** command, the system automatically deletes the statistics and starts collecting statistics again. You can check whether GVRP is running normally on a port by checking the GVRP statistics on it:

- If the number of received GVRP packets and the number of sent GVRP packets are the same as those on the remote port, it indicates that the ports are transmitting and receiving GVRP packets normally and no registration information is lost.
- If the number of dropped GVRP packets is not 0, it indicates that the registration mode on the port may be fixed or forbidden. As in either mode dynamic VLANs cannot be registered, GVRP packet drop may occur on the port.

Examples

Display the GARP statistics on GigabitEthernet1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> display garp statistics interface GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2
        GARP statistics on port GigabitEthernet1/0/1

        Number Of GVRP Frames Received          : 0
        Number Of GVRP Frames Transmitted       : 0
```

```
Number Of Frames Discarded              : 0

GARP statistics on port GigabitEthernet1/0/2

Number Of GVRP Frames Received          : 0
Number Of GVRP Frames Transmitted       : 0
Number Of Frames Discarded              : 0
```

Table 1-1 Description on the fields of the **display garp statistics** command

Field	Description
Number of GVRP Frames Received	Number of the GVRP frames received on the port
Number of GVRP Frames Transmitted	Number of the GVRP frames transmitted through the port
Number of Frames Discarded	Number of GVRP frames discarded by the port

display garp timer

Syntax

display garp timer [**interface** *interface-list*]

View

Any view

Parameters

interface-list: Specifies a list of Ethernet ports of which the GARP timer settings are to be displayed. In this list, you can specify individual ports and port ranges. An individual port takes the form of *interface-type interface-number* and a port range takes the form of *interface-type interface-number1* **to** *interface-type interface-number2*, with *interface-number2* taking a value greater than *interface-number1*. The total number of individual ports and port ranges defined in the list must not exceed 10.

Description

Use the **display garp timer** command to display the settings of the GARP timers on specified ports or all ports.

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

This command displays the settings of the following timers:

- Join timer
- Leave timer
- LeaveAll timer
- Hold timer

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

Examples

Display the settings of the GARP timers on port GigabitEthernet1/0/1.

```
<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
```

garp timer

Syntax

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

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

View

Ethernet port view

Parameters

hold: Sets the GARP Hold timer.

join: Sets the GARP Join timer.

leave: Sets the GARP Leave timer.

timer-value: Timeout time (in centiseconds) of the GARP timer (Hold, Join or Leave) to be set.

Description

Use the **garp timer** command to set a GARP timer (that is, the Hold timer, the Join timer, or the Leaver timer) for an Ethernet port.

Use the **undo garp timer** command to restore the default setting of a GARP timer.

By default, the Hold, Join, and Leave timers are set to 10, 20, and 60 centiseconds.

Note that:

- The setting of each timer must be a multiple of 5 (in centiseconds).
- The timeout ranges of the timers vary depending on the timeout values you set for other timers. If you want to set the timeout time of a timer to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

The following table describes the relations between the timers:

Table 1-2 Relations between the timers

Timer	Lower threshold	Upper threshold
Hold	10 centiseconds	This upper threshold is less than or equal to one-half of the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.
Join	This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.	This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.
Leave	This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.	This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.
LeaveAll	This lower threshold is greater than the timeout time of the Leave timer. You can change threshold by changing the timeout time of the Leave timer.	32,765 centiseconds

Note

In networking, the following GARP timer settings are recommended:

- GARP hold timer: 100 centiseconds (1 second)
- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)

Related commands: **display garp timer**.

Examples

Set the GARP Join timer to 30 centiseconds for GigabitEthernet1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer join 30
```

garp timer leaveall

Syntax

garp timer leaveall *timer-value*

undo garp timer leaveall

View

System view

Parameters

timer-value: Setting (in centiseconds) of the GARP LeaveAll timer. You need to set this argument with the Leave timer settings of other Ethernet ports as references. That is, this argument needs to be larger than the Leave timer settings of any Ethernet ports. Also note that this argument needs to be a multiple of 5 and cannot be larger than 32,765.

Description

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

Use the **undo garp timer leaveall** command to restore the default setting of the GARP LeaveAll timer.

By default, the LeaveAll timer is set to 1,000 centiseconds, that is, 10 seconds.

Note

In networking, you are recommended to set the GARP LeaveAll timer to 12000 centiseconds (2 minutes).

Related commands: **display garp timer**.

Examples

Set the GARP LeaveAll timer to 100 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] garp timer leaveall 100
```

reset garp statistics

Syntax

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

View

User view

Parameters

interface-list: Specifies a list of Ethernet ports. In this list, you can specify individual ports and port ranges. An individual port takes the form of *interface-type interface-number* and a port range takes the form of *interface-type interface-number1* **to** *interface-type interface-number2*, with *interface-number2* taking a value greater than *interface-number1*. The total number of individual ports and port ranges defined in the list must not exceed 10.

Description

Use the **reset garp statistics** command to clear the GARP statistics (including statistics about packets received/sent/discarded by GVRP) on the specified or all ports. You can use the **display garp statistics** command to view the NDP statistics before and after the execution of the **reset garp statistics** command to verify the execution result.

Executing the **reset garp statistics** command without any parameter clears the GARP statistics of all ports.

Related commands: **display garp statistics**.

Examples

Clear GARP statistics of all ports.

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

GVRP Configuration Commands

display gvrp statistics

Syntax

display gvrp statistics [**interface** *interface-list*]

View

Any view

Parameters

interface *interface-list*: Specifies an Ethernet port list. By providing a value for this argument, you can display the GVRP statistics on the specified ports. You need to provide the *interface-list* argument in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where the *interface-type* argument represents the port type, the *interface-number* argument represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Note that, this command displays GVRP statistics only on the trunk ports included in the list. Statistics on non-trunk ports will not be displayed.

Description

Use the **display gvrp statistics** command to display the GVRP statistics of trunk ports.

This command displays the following information:

- GVRP status
- Number of the GVRP entries that fail to be registered
- Source MAC address of the previous GVRP PDU
- GVRP registration type of a port

Examples

Display the GVRP statistics of GigabitEthernet1/0/1, assuming that the port is a trunk port.

```
<Sysname> display gvrp statistics interface GigabitEthernet 1/0/1
        GVRP statistics on port GigabitEthernet1/0/1
```

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

display gvrp status

Syntax

display gvrp status

View

Any view

Parameters

None

Description

Use the **display gvrp status** command to display the global GVRP status (enabled or disabled).

Examples

Display the global GVRP status.

```
<Sysname> display gvrp status
GVRP is enabled
```

The above information indicates that GVRP is enabled globally.

gvrp

Syntax

gvrp

undo gvrp

View

System view, Ethernet port view

Parameters

None

Description

Use the **gvrp** command to enable GVRP globally (in system view) or for a port (in Ethernet port view).

Use the **undo gvrp** command to disable GVRP globally (in system view) or on a port (in Ethernet port view).

By default, GVRP is disabled both globally and on ports.

Note that:

- To enable GVRP for a port, you need to enable GVRP globally first. GVRP does not take effect automatically on ports upon being enabled globally.
- You can enable/disable GVRP only on trunk ports.
- After you enable GVRP on a trunk port, you cannot change the port to other types.

Related commands: **display gvrp status**.

Examples

Enable GVRP globally.

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

Enable GVRP on GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] gvrp
GVRP is enabled on port GigabitEthernet1/0/5.
```

gvrp registration

Syntax

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View

Ethernet port view

Parameters

fixed: Specifies the fixed GVRP registration mode. A port operating in this mode cannot register or deregister VLAN information dynamically. It only propagates static VLAN information. Besides, the port permits only static VLANs, that is, it propagates only static VLAN information to the other GARP members.

forbidden: Specifies the forbidden GVRP registration mode. A port operating in this mode cannot register or deregister VLAN information dynamically. It permits only VLAN 1, that is, it propagates only the information about VLAN 1 to the other GARP members.

normal: Specifies the normal mode. A port operating in this mode can dynamically register or deregister VLAN information and can propagate both dynamic and static VLAN information.

Description

Use the **gvrp registration** command to configure the GVRP registration mode on a port.

Use the **undo gvrp registration** command to restore the default GVRP registration mode on a port.

By default, the GVRP registration mode is **normal**.

Note that these commands only apply to trunk ports.

Related commands: **display gvrp statistics**

Examples

Configure GigabitEthernet1/0/1 to operate in fixed GVRP registration mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] gvrp registration fixed
```

Table of Contents

1 Port Basic Configuration Commands

Port Basic Configuration Commands

broadcast-suppression

Syntax

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

undo broadcast-suppression

View

System view, Ethernet port view

Parameters

ratio: Maximum ratio of the broadcast traffic allowed on a port to the total transmission capacity of the port. The value ranges from 1 to 100 (in step of 1) and defaults to 100. The smaller the ratio is, the less broadcast traffic is allowed.

max-pps: Maximum number of broadcast packets allowed to be received per second on an Ethernet port (in pps). The following are the value ranges for the argument:

- In system view, the value range is 200 to 14881000.
- In Ethernet port view, the value range is 200 to 1488100.

Description

Use the **broadcast-suppression** command to limit broadcast traffic allowed to be received on each port (in system view) or on a specified port (in Ethernet port view).

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

The **broadcast-suppression** command is used to enable broadcast suppression. By default, broadcast suppression is disabled.

When incoming broadcast traffic exceeds the broadcast traffic threshold you set, the system drops the packets exceeding the threshold to reduce the broadcast traffic ratio to the specified range, so as to keep normal network service.

You can use the undo broadcast-suppression command in system view to cancel the broadcast suppression settings on all ports, or use the broadcast-suppression command in system view to make a global setting.

Executing the commands in Ethernet port view only takes effect on the current port.

Note

The global broadcast suppression setting configured by the broadcast-suppression command in system view takes effect on all Ethernet ports in the system except for the reflection ports, stack ports and ports having their own broadcast suppression settings.

If you configure broadcast-suppression command in both system view and Ethernet port view, the configuration in Ethernet port view will take effect.

Examples

Allow incoming broadcast traffic on GigabitEthernet 1/0/1 to occupy at most 20% of the total transmission capacity of the port and suppress the broadcast traffic that exceeds the specified range.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression 20
```

Set the maximum number of broadcast packets that can be received per second by the GigabitEthernet 1/0/1 port to 1,000.

```
[Sysname-GigabitEthernet1/0/1] broadcast-suppression pps 1000
```

copy configuration

Syntax

copy configuration source { *interface-type interface-number* | **aggregation-group** *source-agg-id* } **destination** { *interface-list* [**aggregation-group** *destination-agg-id*] | **aggregation-group** *destination-agg-id* }

View

System view

Parameters

interface-type: Port type.

interface-number: Port number.

source-agg-id: Source aggregation group number, in the range of 1 to 50. The port with the smallest port number in the aggregation group is used as the source port.

destination-agg-id: Destination aggregation group number, in the range of 1 to 50.

interface-list: Destination port list, *interface-list* = *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10. &<1-10> means that you can input up to 10 ports/port ranges.

Description

Use the **copy configuration** command to duplicate the configuration of a port to specified ports to keep consistent configuration on them.

Note

- If you specify a source aggregation group ID, the system uses the port with the smallest port number in the aggregation group as the source.
- If you specify a destination aggregation group ID, the configuration of the source port will be copied to all ports in the aggregation group and all ports in the group will have the same configuration as that of the source port.

Refer to Table 1-1 for the configurations that can be copied.

Table 1-1 Configurations that can be copied

Configuration category	Contents
VLAN	VLANs carried on the port and the default VLAN ID.
Protocol-based VLAN	Protocol VLAN IDs and protocol indexes.
LACP (Link Aggregation Control protocol)	The enable/disable status of LACP. (As the configuration commands of manual and static link aggregation groups cannot be copied, you cannot assign a port to a link aggregation group with the **copy** command.)
QoS	Traffic policing, packet priority marking, port priority, traffic accounting, VLAN mapping, port rate limiting, priority trust mode, QoS profile (the **qos-profile port-based** configuration cannot be copied), and so on.
STP	The enable/disable state of STP on the port, link attribute of the port (point-to-point or non-point-to-point), STP priority, path cost, transmission rate limit, enable/disable state of loop protection, enable/disable state of root protection, and whether the port is an edge port.
GARP	GVRP enable/disable status, timer settings, and registration mode.
Basic port configuration	Link type of the port, port rate, and duplex mode.

In case a configuration setting fails to be copied, the system will print the error message.

Examples

Copy the configurations of GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] copy configuration source GigabitEthernet 1/0/1 destination GigabitEthernet 1/0/2
GigabitEthernet 1/0/3
 Note: The following will be removed from destination port list:
 Aggregation port(s), Voice vlan port(s).
 Copying VLAN configuration...
 Copying Protocol based VLAN configuration...
 Copying LACP configuration...
 Copying QOS configuration...
 Copying GARP configuration...
```

```
Copying STP configuration...
Copying speed/duplex configuration...
```

 **Note**

- Any aggregation group port you input in the destination port list will be removed from the list and the **copy** command will not take effect on the port. If you want an aggregation group port to have the same configuration with the source port, you can specify the aggregation group of the port as the destination (with the *destination-agg-id* argument).
- Any voice-VLAN-enabled port you input in the destination port list will be removed from the list.

Copy the configurations of GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2.

```
[Sysname]copy configuration source GigabitEthernet 1/0/1 destination GigabitEthernet 1/0/2
 Copying VLAN configuration...
 Copying Protocol based VLAN configuration...
 Copying LACP configuration...
 Copying QOS configuration...
 Copying GARP configuration...
 Copying STP configuration...
 Copying speed/duplex configuration...
 Copying speed configuration to interface GigabitEthernet1/0/2 failed
 Copying QoS rate limit configuration to interface GigabitEthernet1/0/2 failed
```

The output shows that all configurations except port rate limiting and QoS traffic policing were copied successfully.

description

Syntax

description *text*

undo description

View

Ethernet port view

Parameters

text: Port description, a string of 1 to 80 characters.

Description

Use the **description** command to configure a description for the port.

Use the **undo description** command to remove the port description.

By default, no description is configured for a port.

You can use the **display brief interface** command to display the configured description.

Examples

Set description string **home** for the GigabitEthernet 1/0/1 port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description home
```

display brief interface

Syntax

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

View

Any view

Parameters

interface-type: Port type.

interface-number: Port number.

|: Specifies to use a regular expression to filter the configuration information entries to be displayed.

begin: Each entry must begin with a specified character string.

include: Each entry must include a specified character string.

exclude: Each entry must not include a specified character string.

regular-expression: Regular expression, a string of 1 to 256 characters.

 **Note**

For details about regular expression, refer to the Configuration File Management module in this manual.

Description

Use the **display brief interface** command to display the brief configuration information about one or all interfaces, including: interface type, link state, link rate, duplex attribute, link type, default VLAN ID and description string.

 **Note**

Currently, for the port types other than Ethernet port, this command only displays the link state, and shows "--" in all other configuration information fields.

Related commands: **display interface**.

Examples

Display the brief configuration information about the GigabitEthernet 1/0/1 port.

```
<Sysname> display brief interface GigabitEthernet 1/0/1
Interface:
Eth  - Ethernet  GE   - GigabitEthernet TENGE - tenGigabitEthernet
Loop - LoopBack  Vlan - Vlan-interface  Cas   - Cascade
Speed/Duplex:
A - auto-negotiation

Interface   Link     Speed  Duplex Type   PVID Description
------------------------------------------------------------------------
GE1/0/1     DOWN     A      A      hybrid 1    home
```

Table 1-2 Description on the fields of the **display brief interface** command

Field	Description
Interface	Port type
Link	Current link state: UP, DOWN or ADMINISTRATIVELY DOWN
Speed	Link rate
Duplex	Duplex attribute
Type	Link type: access, hybrid or trunk
PVID	Default VLAN ID
Description	Port description string

The state of an Ethernet port can be UP, DOWN, or ADMINISTRATIVELY DOWN. The following table shows the port state transitions.

Table 1-3 Port state transitions

Initial port state		State after executing the shutdown command	State after executing the undo shutdown command
Not connected to any cable	DOWN	ADMINISTRATIVELY DOWN	DOWN
	ADMINISTRATIVELY DOWN		DOWN
Connected to a cable	DOWN		DOWN
	UP		UP
	ADMINISTRATIVELY DOWN		UP

display interface

Syntax

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

View

Any view

Parameters

interface-type: Port type.

interface-number: Port number.

For details about the arguments, refer to the parameter description of the **interface** command.

Description

Use the **display interface** command to display port configuration.

When using this command:

- If you specify neither port type nor port number, the command displays information about all ports.
- If you specify only port type, the command displays information about all ports of the specified type.
- If you specify both port type and port number, the command displays information about the specified port.

Examples

Display the configuration information of GigabitEthernet 1/0/1.

```
<Sysname> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state : DOWN
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc00-5190
 Media type is twisted pair, loopback not set
 Port hardware type is 1000_BASE_T
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unknown Multicast Packet drop: Disable
 Unknown Unicast Packet drop: Disable
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Last 300 seconds input:  0 packets/sec 0 bytes/sec
 Last 300 seconds output:  0 packets/sec 0 bytes/sec
 Input(total):  0 packets, - bytes
          - broadcasts, - multicasts, - pauses
 Input(normal):  0 packets, 0 bytes
          0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants,  - throttles, 0 CRC
          0 frame,  0 overruns, 0 aborts, - ignored, - parity errors
 Output(total): 0 packets, - bytes
          - broadcasts, - multicasts, - pauses
```

```
Output(normal): 0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors,  - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

Table 1-4 Description on the fields of the **display interface** command

Field	Description
GigabitEthernet1/0/1 current state	Current GigabitEthernet port status: UP, DOWN or ADMINISTRATIVELY DOWN
IP Sending Frames' Format	Ethernet frame format
Hardware address	Port hardware address
Media type	Media type
Port hardware type	Port hardware type
Unknown-speed mode, unknown-duplex mode	Current speed mode and duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation	Link speed and duplex status (force or auto-negotiation)
Flow-control is not enabled	Status of flow-control on the port
The Maximum Frame Length	Maximum frame length allowed on the port
Broadcast MAX-ratio	Broadcast suppression ratio on the port
Allow jumbo frame to pass	Whether Jumbo frame is allowed on the port.
PVID	Default VLAN ID of the port
Mdi type	Network cable type
Port link-type	Port link type
Tagged VLAN ID	Identify the VLANs whose packets will be forwarded with tags on the port.
Untagged VLAN ID	Identify the VLANs whose packets will be forwarded without tags on the port.
Last 300 seconds input: 0 packets/sec 0 bytes/sec Last 300 seconds output: 0 packets/sec 0 bytes/sec	Average input and output rates (in pps and Bps) in the last 300 seconds
Input(total): 0 packets, 0 bytes 0 broadcasts, 0 multicasts, 0 pauses	Count in packets and in bytes of total incoming traffic on the port, including incoming normal packets, abnormal packets, and normal PAUSE frames The number of incoming broadcast packets, the number of incoming multicast packets, and the number of incoming PAUSE frames on the port.

Field	Description
Input(normal): - packets, - bytes - broadcasts, - multicasts, - pauses	Count in packets and in bytes of incoming normal packets on the port, including incoming normal packets and normal PAUSE frames The number of normal incoming broadcast packets, the number of normal incoming multicast packets, and the number of normal incoming PAUSE frames of the port A hyphen (-) indicates that the statistical item is not supported
input errors	The total number of incoming error frames
runts	The number of incoming runt frames A runt frame is of less than 64 bytes but has the correct format and CRC field
giants	The number of incoming giant frames (A giant frame is of more than 1518 bytes if untagged or more than 1522 bytes if tagged.)
- throttles	The number of throttles that occurred on the port (A throttle occurs when a port is shut down due to buffer or memory overload.)
CRC	The number of CRC error frames received in correct length
frame	The number of incoming CRC error frames with non-integer number of bytes
- overruns	The number of packets dropped because the receiving rate of the port exceeds the processing capability of the input queues
aborts	The total number of incoming illegal packets, including: • Fragments: CRC error frames of less than 64 bytes (integer or non-integer). • Jabber frames: CRC error frames of more than 1518 bytes if untagged or 1522 bytes if tagged (integer or non-integer). • Symbol error frames: frames with at least one symbol error. • Unknown operator frames: MAC control frames that are not Pause frames • Length error frames: frames whose actual length (46-1500 bytes) is inconsistent with the length field in the 802.3 header.
ignored	The number of packets dropped due to insufficient receive buffer on the port
- parity errors	The number of incoming parity error frames
Output(total): 0 packets, - bytes - broadcasts, - multicasts, - pauses	Count in packets and in bytes of total outgoing traffic on the port, including normal packets, abnormal packets, and normal Pause frames The number of outgoing broadcast packets, the number of outgoing multicast packets, and the number of outgoing Pause frames on the port A hyphen (-) indicates that the statistical item is not supported.

Field	Description
Output(normal): 0 packets, 0 bytes 0 broadcasts, 0 multicasts, 0 pauses	Count in packets and in bytes of outgoing normal packets on the port, including outgoing normal packets and normal Pause frames. The number of normal outgoing broadcast packets, the number of normal outgoing multicast packets, and the number of normal outgoing Pause frames on the port.
output errors	The total number of outgoing error frames
- underruns	The number of packets dropped because the transmitting rate of the port exceeds the processing capacity of the output queue, which is a rare hardware error.
- buffer failures	The number of packets dropped due to insufficient transmit buffer on the port
aborts	The number of transmission failures due to various reasons, such as collisions
deferred	The number of first transmission attempts delayed because of detection of collisions
collisions	The number of detected collisions (Transmission of a frame will be aborted upon detection of a collision.)
late collisions	The number of detected late collisions (A late collision occurs if the transmission of a frame defers due to detection of collision after its first 512 bits have been transmitted.)
lost carrier	The lost carrier counter applicable to serial WAN interfaces The counter increases by 1 upon each carrier loss detected during frame transmission.
- no carrier	The no carrier counter applicable to serial WAN interfaces The counter increases by 1 upon each carrier detection failure for frame transmission.

display link-delay

Syntax

display link-delay

View

Any view

Parameters

None

Description

Use the **display link-delay** command to display the information about the ports with the **link-delay** command configured, including the port name and the configured delay.

Related commands: **link-delay**.

Examples

Display the information about the ports with the **link-delay** command configured.

```
<Sysname> display link-delay
 Interface               Time Delay
 ====================== ==============
 GigabitEthernet1/0/5          8
```

display loopback-detection

Syntax

display loopback-detection

View

Any view

Parameters

None

Description

Use the **display loopback-detection** command to display the loopback detection status on the port. If loopback detection is enabled, this information will also be displayed: time interval for loopback detection and the loopback ports.

Examples

Display the loopback detection status on the port.

```
<Sysname> display loopback-detection
 Port GigabitEthernet1/0/1 loopback-detection is running
 system Loopback-detection is running
 Detection interval time is 30 seconds
 There is no port existing loopback link
```

Table 1-5 Description on the fields of the **display loopback-detection** command

Field	Description
Port GigabitEthernet1/0/1 loopback-detection is running	Loopback detection is enabled on the GigabitEthernet 1/0/1.
system Loopback-detection is running	Loopback detection is enabled globally.
Detection interval time is 30 seconds	Time interval for loopback detection is 30 seconds.
There is no port existing loopback link	No loopback port exists.

display port combo

Syntax

display port combo

View

Any view

Parameters

None

Description

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

Examples

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

```
<Sysname> display port combo
Combo-group       Active                    Inactive
       1       GigabitEthernet1/0/23      GigabitEthernet1/0/49
       2       GigabitEthernet1/0/24      GigabitEthernet1/0/50
       3       GigabitEthernet1/0/47      GigabitEthernet1/0/51
       4       GigabitEthernet1/0/48      GigabitEthernet1/0/52
```

Table 1-6 display port combo command output description

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

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

display port-group

Syntax

display port-group *group-id*

View

Any view

Parameter

group-id: Number of port group, in the range of 1 to 100.

Description

Use the **display port-group** command to display information for a specified port group .

Example

Display information for the port group 1.

```
<Sysname> display port-group 1
Port Group 1:
  Interface list: GigabitEthernet1/0/2-5
```

The above information indicates that port group 1 includes 4 ports: from GigabitEthernet1/0/2 to GigabitEthernet1/0/5.

display storm-constrain

Syntax

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

View

Any view

Parameters

interface-type: Port type.

interface-number: Port number.

|: Uses a regular expression to filter the output configuration information.

begin: Displays the configurations that begin with the string specified by *regular-expression*.

exclude: Displays the configurations that do not contain the string specified by *regular-expression*.

include: Displays the configurations that contain the string specified by *regular-expression*.

regular-expression: Regular expression.

Description

Use the **display storm-constrain** command to display the storm control configurations.

Examples

Display the storm control configurations.

```
<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
------------------------------------------------------------------------------
GE1/0/5       BC   1          1          NA       normal  on   on  0      pps
```

Table 1-7 Description on the fields of the **display storm-constrain** command

Field	Description
Flow Statistic Interval	Interval to collect traffic statistics.
PortName	Name of an Ethernet port
Type	Traffic type, which can be unicast, multicast, and broadcast
LowerLimit	Lower threshold of traffic received on the port
UpperLimit	Upper threshold of traffic received on the port
CtrMode	Control action to be taken when the broadcast/multicast/unicast traffic exceeds the upper threshold, which can be block or shutdown.
Status	Current status of the port, which can be normal or control.
Trap	on: trap information is output when a type of traffic received on the port exceeds the upper threshold or falls below the lower threshold. off: trap information is not output when a type of traffic received on the port exceeds the upper threshold or falls below the lower threshold.
Log	on: log information is output when traffic received on the port exceeds the upper threshold or falls below the lower threshold off: log information is not output when traffic received on the port exceeds the upper threshold or falls below the lower threshold
SwiNum	Number of port state switchover

display unit

Syntax

display unit *unit-id* **interface**

View

Any view

Parameters

unit-id: Unit ID, only can be 1.

Description

Use the **display unit** command to display information about the ports on a specified unit.

Examples

Display information about the ports on unit 1.

```
<Sysname> display unit 1 interface
Aux1/0/0
Description :  Aux Interface
 GigabitEthernet1/0/1 current state : DOWN
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc00-5190
 Media type is twisted pair, loopback not set
 Port hardware type is 1000_BASE_T
```

```
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-ratio: 100%
Unknown Multicast Packet drop: Disable
Unknown Unicast Packet drop: Disable
Allow jumbo frame to pass
PVID: 1
Mdi type: auto
Port link-type: access
 Tagged   VLAN ID : none
 Untagged VLAN ID : 1
Last 300 seconds input:  0 packets/sec 0 bytes/sec
Last 300 seconds output:  0 packets/sec 0 bytes/sec
Input(total):  0 packets, - bytes
         - broadcasts, - multicasts, - pauses
Input(normal):  0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants,  - throttles, 0 CRC
         0 frame,  0 overruns, 0 aborts, - ignored, - parity errors
Output(total): 0 packets, - bytes
         - broadcasts, - multicasts, - pauses
Output(normal): 0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors,  - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

(The following displayed information is omitted)

Table 1-8 Description on the fields of the **display unit** command

Field	Description
Aux1/0/0 Description : Aux Interface	The description string of the AUX port is **Aux Interface**.

For the description of other fields, refer to Table 1-4.

duplex

Syntax

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

undo duplex

View

Ethernet port view

Parameters

auto: Sets the port to auto-negotiation mode.

full: Sets the port to full duplex mode.

half: Sets the port to half duplex mode.

Description

Use the **duplex** command to set the duplex mode of the current port.

Use the **undo duplex** command to restore the default duplex mode, that is, auto-negotiation.

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

Related commands: **speed**.

Examples

Set the GigabitEthernet 1/0/1 port to auto-negotiation mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex auto
```

enable log updown

Syntax

enable log updown

undo enable log updown

View

Ethernet port view

Parameters

None

Description

Use the **enable log updown** command to enable Up/Down log information output.

Use the **undo log enable updown** command to disable Up/Down log information output.

By default, a port is allowed to output Up/Down log information.

Examples

By default, a port is allowed to output the Up/Down log information. Execute the **shutdown** command or the **undo shutdown** command on GigabitEthernet 1/0/1, and the system outputs Up/Down log information of GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1]
```

```
%Apr  5 07:25:37:634 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is DOWN
[Sysname-GigabitEthernet1/0/1] undo shutdown
[Sysname-GigabitEthernet1/0/1]
%Apr  5 07:25:56:244 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is UP
```

Disable GigabitEthernet 1/0/1 from outputting Up/Down log information and execute the **shutdown** command or the **undo shutdown** command on GigabitEthernet 1/0/1. No Up/Down log information is output for GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] undo enable log updown
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

flow-control

Syntax

flow-control

undo flow-control

View

Ethernet port view

Parameters

None

Description

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

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

Suppose flow control is enabled on both the local and peer switches. When congestion occurs on the local switch,

the local switch sends a message to notify the peer switch of stopping sending packets to itself or reducing the sending rate temporarily,

the peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

By default, flow control is disabled on a port.

Examples

Enable flow control on the GigabitEthernet 1/0/1 port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

flow interval

Syntax

flow-interval *interval*

undo flow-interval

View

Ethernet port view

Parameters

Interval: Interval (in seconds) to perform statistics on port information. This argument ranges from 5 to 300 (in step of 5) and is 300 by default.

Description

Use the **flow-interval** command to set the interval to perform statistics on port information.

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

By default, this interval is 300 seconds.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set the interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input:  0 packets/sec 0 bytes/sec
Last 100 seconds output:  0 packets/sec 0 bytes/sec
```

Related commands: **display interface**.

Examples

Set the interval to perform statistics on the GigabitEthernet 1/0/1 port to 100 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

interface

Syntax

interface *interface-type interface-number*

View

System view

Parameters

interface-type: Port type, which can be Aux, GigabitEthernet, TenGigabitEthernet .LoopBack, NULL or VLAN-interface.

interface-number: Port number. For the GigabitEthernet and TenGigabitEthernet port, it is in the format of slot number/subslot number/port number.

- The slot number is fixed to 1;
- The subslot number is 0 if the port is an GigabitEthernet port, the subslot number is 1 or 2 if the port is a TenGigabitEthernet port;
- The port number is relevant to the device.

Description

Use the **interface** command to enter specific port view. To configure an Ethernet port, you need to enter Ethernet port view first.

Examples

Enter GigabitEthernet 1/0/1 port view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

jumboframe enable

Syntax

jumboframe enable

undo jumboframe enable

View

Ethernet port view

Parameters

None

Description

Use the **jumboframe enable** command to set the maximum frame size allowed on a port to 9,216 bytes.

Use the **undo jumboframe enable** command to set the maximum frame size allowed on a port to 1,522 bytes.

By default, the maximum frame size allowed on an Ethernet port is 9,216 bytes.

Examples

Set the maximum frame size allowed on GigabitEthernet 1/0/1 to 9.216 bytes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

link-delay

Syntax

link-delay *delay-time*

undo link-delay

View

Ethernet port view

Parameters

delay-time: Port state change delay to be set. This argument is in the range 2 to 10 (in seconds).

Description

Use the **link-delay** command to set the port state change delay.

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

By default, the port state change delay is 0 seconds, that is, the port state changes without any delay.

During a short period after you connect your switch to another device, the connecting port may go up and down frequently due to hardware compatibility, resulting in service interruption.

To avoid situations like this, you may set a port state change delay.

 **Note**

- The port state change delay takes effect when the port goes down but not when the port goes up.
- The delay configured in this way does not take effect for ports in DLDP down state. For information about the DLDP down state, refer to *DLDP*.

Examples

Set the port state change delay of GigabitEthernet 1/0/5 to 8 seconds.

```
<Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/5
[Sysname-GigabitEthernet1/0/5] link-delay 8
```

loopback

Syntax

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

View

Ethernet port view

Parameters

external: Performs external loop test. In the external loop test, self-loop headers must be used on the port of the switch. The external loop test can locate the hardware failures on the port.

Note

For 1000M port, the self-loop headers are made from eight cores of the 8-core cables, and the packets forwarded by the port will be received by itself.

internal: Performs internal loop test. In the internal loop test, self loop is established in the switching chip to locate the chip failure which is related to the port.

Description

Use the **loopback** command to perform a loopback test on the current Ethernet port to check whether the Ethernet port works normally. The loopback test terminates automatically after running for a specific period.

By default, no loopback test is performed on the Ethernet port.

Examples

Perform an internal loop test on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
 Loopback internal succeeded.
```

loopback-detection control enable

Syntax

loopback-detection control enable

undo loopback-detection control enable

View

Ethernet port view

Parameters

None

Description

Use the **loopback-detection control enable** command to enable the loopback detection control feature on the current trunk or hybrid port.

Use the **undo loopback-detection control enable** command to disable the loopback detection control feature on the trunk or hybrid port.

This function needs to be used in conjunction with the loopback detection function. For details, refer to the **loopback-detection enable** command. When a loopback is detected in a VLAN on a trunk or hybrid port, you can use this function to control the working status of the port.

- If this feature is enabled on a trunk or hybrid port, when loopback is found on the port, the system puts the port into the controlled working status and removes the MAC address entries corresponding to the port.
- If this feature is disabled on a trunk or hybrid port, when loopback is found on the port, the system just reports a Trap message, and the port still works normally.

By default, the loopback detection control feature is disabled on the trunk or hybrid port.

Note that this command is invalid for an access port.

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

Examples

Enable the loopback detection control feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] loopback-detection control enable
```

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

System view or Ethernet port view

Parameters

None

Description

Use the **loopback-detection enable** command to enable the loopback detection feature on ports to detect whether external loopback occurs on a port.

Use the **undo loopback-detection enable** command to disable the loopback detection feature on port.

- If loopback is found on an access port, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.
- If loopback is found on a trunk or hybrid port, the system sends a Trap message to the client. If the loopback port control function is enabled on the port (with the **loopback-detection control enable** command), the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.

Note

The loopback detection feature takes effect on a port only when the loopback detection feature is enabled in both system view and the specified port view.

By default, the loopback detection feature is disabled on any port.

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

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
```

loopback-detection *interface-list* enable

Syntax

loopback-detection *interface-list* **enable**

undo loopback-detection *interface-list* **enable**

View

System view

Parameter

interface-list: Ethernet port list, in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where

- *interface-type* is the port type, and *interface-number* is the port number.
- Keyword **to** is used to specify a range of ports. The port number after **to** must be equal to or greater than that before **to**.
- &<1-10> means that you can specify up to 10 ports or port ranges.

Description

Use the **loopback-detection** *interface-list* **enable** command to enable the loopback detection function on a range of ports.

Use the **undo loopback-detection** *interface-list* **enable** command to disable the loopback detection function on a range of ports.

Example

Enable the loopback detection function on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] loopback-detection enable
[Sysname] loopback-detection GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4 enable
```

loopback-detection interval-time

Syntax

loopback-detection interval-time *time*

undo loopback-detection interval-time

View

System view

Parameters

time: Time interval for loopback detection, in the range of 5 to 300 (in seconds). It is 30 seconds by default.

Description

Use the **loopback-detection interval-time** command to set time interval for loopback detection.

Use the **undo loopback-detection interval-time** command to restore the default time interval.

Examples

Set time interval for loopback detection to 10 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] loopback-detection interval-time 10
```

loopback-detection per-vlan enable

Syntax

loopback-detection per-vlan enable

undo loopback-detection per-vlan enable

View

Ethernet port view

Parameters

None

Description

Use the **loopback-detection per-vlan enable** command to configure the system to run loopback detection on all VLANs of the current trunk or hybrid port.

Use the **undo loopback-detection per-vlan enable** command to restore the default setting.

By default, the system runs loopback detection only on the default VLAN of the trunk or hybrid port.

Note that, this command is not applicable to access ports. When the link type of a non-access port changes to access, the **loopback-detection per-vlan enable** command already configured on the port becomes invalid automatically.

Examples

Configure the system to run loopback detection on all VLANs of the trunk port GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

```
[Sysname-GigabitEthernet1/0/1] loopback-detection per-vlan enable
```

mdi

Syntax

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

undo mdi

View

Ethernet port view

Parameters

across: Sets the MDI mode to medium dependent interface (MDI).

normal: Sets the MDI mode to media dependent interface-X mode (MDI-X).

auto: Sets the MDI mode to auto-sensing. Port operating in this mode adjust its MDI mode between MDI and MDI-X automatically.

 **Note**

- An RJ-45 interface can operate in MDI or MDI-X mode.
- To connect two RJ-45 interfaces operating in the same MDI mode, use a crossover cable; to connect two RJ-45 interfaces operating in different MDI modes, use a straight-through cable.
- The MDI mode of an optical port is fixed to **auto**.

Description

Use the **mdi** command to set the MDI mode for a port.

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

By default, a port operates in auto-sensing MDI mode.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mdi across
```

port-group

Syntax

port-group *group-id*

undo port-group *group-id*

View

System view

Parameter

group-id: Number of port group, in the range of 1 to 100.

Description

Use the **port-group** command to create a port group or enter the specified port group view.

By default, no port group is configured.

Example

Create port group 1.

```
<Sysname> system-view
[Sysname] port-group 1
[Sysname-port-group-1]
```

port

Syntax

port *interface-list*

undo port *interface-list*

View

Port group view

Parameter

interface-list: Ethernet interface 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.

Description

Use the **port** command to add Ethernet interface(s) to a specified port group.

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

By default, a port group is empty, that is, there is no Ethernet interface in it.

Example

Add the interface GigabitEthernet 1/0/2~GigabitEthernet1/0/5 to the port group1.

```
<Sysname> system-view
[Sysname] port-group 1
[Sysname-port-group-1] port GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5
```

reset counters interface

Syntax

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

View

User view

Parameters

interface-type: Port type.

interface-number: Port number.

For details about the parameters, see the parameter description of the **interface** command.

Description

Use the **reset counters interface** command to clear the statistics of the port, preparing for a new statistics collection.

If you specify neither port type nor port number, the command clears statistics of all ports.

If specify only port type, the command clears statistics of all ports of this type.

If specify both port type and port number, the command clears statistics of the specified port.

Note that the statistics of the 802.1x-enabled ports cannot be cleared.

Examples

Clear the statistics of GigabitEthernet 1/0/1.

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

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet port view

Parameters

None

Description

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

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

By default, an Ethernet port is in up state.

Examples

Shut down GigabitEthernet 1/0/1 and then bring it up.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
#Apr  2 08:33:19:669 2000 Sysname L2INF/2/PORT LINK STATUS CHANGE:- 1 -
```

```
 Trap 1.3.6.1.6.3.1.1.5.3(linkDown): portIndex is 4227745, ifAdminStatus is 1, i
fOperStatus is 2

%Apr  2 08:33:19:860 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is DOWN

%Apr  2 08:33:19:973 2000 Sysname L2INF/5/VLANIF LINK STATUS CHANGE:- 1 -
 Vlan-interface1 is DOWN

%Apr  2 08:33:20:091 2000 Sysname IFNET/5/UPDOWN:- 1 -Line protocol on the interface
 Vlan-interface1 is DOWN
```

Enable GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] undo shutdown
#Apr  2 08:34:06:865 2000 Sysname L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.4(linkUp): portIndex is 4227745, ifAdminStatus is 1, ifO
perStatus is 1
%Apr  2 08:34:07:058 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is UP

%Apr  2 08:34:07:176 2000 Sysname L2INF/5/VLANIF LINK STATUS CHANGE:- 1 -
 Vlan-interface1 is UP

%Apr  2 08:34:07:288 2000 Sysname IFNET/5/UPDOWN:- 1 -Line protocol on the interface
 Vlan-interface1 is UP
```

speed

Syntax

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

undo speed

View

Ethernet port view

Parameters

10: Specifies the port speed to 10 Mbps.

100: Specifies the port speed to 100 Mbps.

1000: Specifies the port speed to 1,000 Mbps.

auto: Specifies the port speed to the auto-negotiation mode.

Description

Use the **speed** command to set the port speed.

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

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

Related commands: **duplex**.

Note

The **speed** and **undo speed** commands cannot be configured on a combo port.

Examples

Set the speed of GigabitEthernet 1/0/1 to 10 Mbps.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed 10
```

speed auto

Syntax

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

View

Ethernet port view

Parameters

10: Configures 10 Mbps as an auto-negotiation speed of the port.

100: Configures 100 Mbps as an auto-negotiation speed of the port.

1000: Configures 1,000 Mbps as an auto-negotiation speed of the port.

Description

Use the **speed auto** [**10** | **100** | **1000**]* command to configure auto-negotiation speed(s) for the current port.

By default, the port speed is auto-negotiated.

The last configuration will take effect if you configure the command for multiple times.

Examples

Configure 10 Mbps and 1000 Mbps as the auto-negotiation speeds of GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto 10 1000
```

storm-constrain

Syntax

storm-constrain broadcast *max-packets min-packets* { **pps** | **kbps** }

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

View

Ethernet port view

Parameters

broadcast: Specifies to control broadcast traffic on the port.

all: Cancels all the storm control threshold configurations on the port.

pps: Specifies the storm constrain threshold in packets.

kbps: Specifies the storm constrain threshold in kilobits per second (kbps).

max-packets: Upper threshold of the traffic on the port, in pps, or kbps. It ranges from 1 to 4,294,967,295 and must be greater than or equal to the lower threshold.

min-packets: Lower threshold of the traffic on the port, in pps, or kbps. It ranges from 1 to 4,294,967,295, and must be less than or equal to the upper threshold.

Description

Use the **storm-constrain** command to set the upper and lower thresholds of the broadcast traffic received on the port.

Use the **undo storm-constrain** command to cancel the threshold configuration.

- With traffic upper and lower thresholds specified on a port, the system periodically collects statistics about the broadcast traffic on the port. Once it finds that a type of traffic exceeds the specified upper threshold, it blocks this type of traffic on the port or directly shuts down the port, and outputs trap/log information according to your configuration.
- When a type of traffic on the port falls back to the specified lower threshold, the system cancels the blocking of this type of traffic on the port or brings up the port to restore traffic forwarding for the port, and outputs log/trap information according to your configuration.

Related commands: **display storm-constrain**, **storm-constrain control**, **storm-constrain enable**.

Examples

Set the upper and lower thresholds of broadcast traffic on GigabitEthernet 1/0/1 to 100 pps and 10 pps respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast 100 10 pps
```

storm-constrain control

Syntax

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

undo storm-constrain control

View

Ethernet port view

Parameters

block: Blocks and stops forwarding those types of traffic exceeding the upper thresholds.

shutdown: Shutdowns the port if the broadcast traffic exceeds the upper threshold, and stops receiving and forwarding all types of traffic on the port.

Description

Use the **storm-constrain control** command to set the action to be taken when the broadcast traffic on the port exceeds the upper threshold.

Use the **undo storm-constrain control** command to cancel the configured action.

By default, no action is taken.

Note

- If the **broadcast-suppression** command is configured on a port, you cannot configure the storm control function on the port, and vice versa.
- You are not recommended to set the upper and lower traffic thresholds to the same value.
- The system can take one of the actions when the broadcast traffic received on a port exceeds the upper threshold: **block** and **shutdown**. The **block** action blocks only those types of traffic that exceed the upper thresholds instead of all types of traffic. When a type of traffic is blocked, it is still counted by the system and contained in the traffic statistics. The **shutdown** action automatically shutdowns the port when a type of traffic on the port exceeds the upper threshold. If you want to bring up the port again, you can execute the **undo shutdown** command or the **undo storm-constrain broadcast** command.

Related commands: **display storm-constrain**, **storm-constrain**.

Examples

Set the control action on GigabitEthernet 1/0/1 to block.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

storm-constrain enable

Syntax

storm-constrain enable { **log** | **trap** }

undo storm-constrain enable

View

Ethernet port view

Parameters

log: Enables log information to be output when traffic received on the port exceeds the upper threshold or falls below the lower threshold.

trap: Enables trap information to be output when traffic received on the port exceeds the upper threshold or falls below the lower threshold.

Description

Use the **storm-constrain enable** command to enable log/trap information to be output when traffic received on the port exceeds the upper threshold or falls below the lower threshold.

Use the **undo storm-constrain enable** command to disable log/trap information from being output when traffic received on the port exceeds the upper threshold or falls below the lower threshold.

By default, log/trap information is output when traffic received on the port exceeds the upper threshold or falls below the lower threshold.

Related commands: **display storm-constrain**, **storm-constrain**.

Examples

Disable log information from being output when traffic received on GigabitEthernet 1/0/1 exceeds the upper threshold or falls below the lower threshold.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo storm-constrain enable log
```

storm-constrain interval

Syntax

storm-constrain interval *interval-value*

undo storm-constrain interval

View

System view

Parameters

interval-value: Interval to collect traffic statistics, in the range of 1 to 300 (in seconds).

Description

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

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

By default, the interval is 10 seconds.

Related commands: **display storm-constrain**, **storm-constrain**.

Examples

Set the interval to collect traffic statistics to 2 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] storm-constrain interval 2
```

virtual-cable-test

Syntax

virtual-cable-test

View

Ethernet port view

Parameters

None

Description

Use the **virtual-cable-test** command to enable the system to test the cable connected to a specific port and to display the results. The system can test these attributes of the cable:

- Cable status, including normal, abnormal, abnormal-open, abnormal-short and failure
- Cable length

 **Note**

- If the cable is in normal state, the displayed length value is the total length of the cable.
- If the cable is in any other state, the displayed length value is the length from the port to the faulty point.

The testing functions that are available on an switch vary with port state as follows:

- For ports that are Down, the cable status testing and cable length testing are available.
- For ports that are Up, the cable status testing, cable length testing, and Pair skew testing are available.

- Pair impedance mismatch
- Pair skew
- Pair swap
- Pair polarity
- Insertion loss
- Return loss
- Near-end crosstalk

By default, the system does not test the cable connected to the Ethernet port.

Note

- Optical port (including Combo optical port) does not support VCT (**virtual-cable-test**) function.
- Combo electrical port supports VCT function only when it is in UP condition (using undo shutdown command), normal Ethernet electrical port always supports this function.
- A hyphen (-) indicates that the corresponding test item is not supported.

Examples

Enable the system to test the cable connected to GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status: normal, 6 metres
Pair Impedance mismatch: -
Pair skew: 8 ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Table of Contents

1 Link Aggregation Configuration Commands

Link Aggregation Configuration Commands

display link-aggregation interface

Syntax

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

View

Any view

Parameters

interface-type: Port type.

interface-number: Port number.

to: Specifies a port index range, with the two *interface-type interface-number* argument pairs around it as the two ends.

Description

Use the **display link-aggregation interface** command to display the link aggregation details about a specified port or port range.

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values.

Examples

Display the link aggregation details on GigabitEthernet 1/0/1.

```
<Sysname> display link-aggregation interface GigabitEthernet1/0/1

 GigabitEthernet1/0/1:
   Selected AggID: 1
   Local:
     Port-Priority: 32768, Oper key: 2, Flag: 0x45
   Remote:
     System ID: 0x8000, 0000-0000-0000
     Port Number: 0, Port-Priority: 32768 , Oper-key: 0, Flag: 0x38
   Received LACP Packets: 0 packet(s), Illegal: 0 packet(s)
   Sent LACP Packets: 0 packet(s)
```

Table 1-1 Description on the fields of the **display link-aggregation interface** command

Field	Description
Selected AggID	ID of the aggregation group to which the specified port belongs
Local	Information about the local end
Port-Priority	Port priority
Oper key	Operation key
Flag	Protocol status flag
Remote	Information about the remote end
System ID	Remote device ID
Port number	Port number
Received LACP Packets: 0 packet(s), Illegal: 0 packet(s) Sent LACP Packets: 0 packet(s)	Statistics about received, invalid, and sent LACP packets

display link-aggregation summary

Syntax

display link-aggregation summary

View

Any view

Parameters

None

Description

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

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values.

Examples

Display summary information of all aggregation groups.

```
<Sysname> display link-aggregation summary

Aggregation Group Type:D -- Dynamic, S -- Static , M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 000f-e20f-5104

  AL  AL   Partner ID           Select Unselect Share Master
  ID  Type                        Ports  Ports     Type  Port
```

```
--------------------------------------------------------------------------
  1   S    0x8000,0000-0000-0000     0    1    NonS  GigabitEthernet1/0/2
  2   M    none                        0    1     NonS  GigabitEthernet1/0/3
```

Table 1-2 Description on the fields of the **display link-aggregation summary** command

Field	Description
Aggregation Group Type	Aggregation group type: D for dynamic, S for static, and M for manual
Loadsharing Type	Load sharing type: Shar for load sharing and NonS for non-load sharing
Actor ID	Local device ID
AL ID	Aggregation group ID
AL Type	Aggregation group type: D (dynamic), S (static), or M (manual)
Partner ID	ID of the remote device, including the system priority and system MAC address of the remote device For a device belonging to an dynamic aggregation group or static aggregation group, if no LACP packet is received, the partner ID is displayed as 0x8000, 0000-0000-0000.
Select Ports	Number of the selected ports
Unselect Ports	Number of the unselected ports
Share Type	Load sharing type: Shar (load-sharing), or NonS (non-load-sharing)
Master Port	the smallest port number in an aggregation group

display link-aggregation verbose

Syntax

display link-aggregation verbose [*agg-id*]

View

Any view

Parameters

agg-id: Aggregation group ID, which ranges from 1 to 50 and must be the ID of an existing aggregation group.

Description

Use the **display link-aggregation verbose** command to display the details about a specified aggregation group or all aggregation groups.

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values.

Examples

Display the details about aggregation group 1.

```
<Sysname> display link-aggregation verbose 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation ID: 1,  AggregationType: Manual,   Loadsharing Type: NonS
Aggregation Description:
System ID: 0x8000, 000f-e214-000a
Port Status: S -- Selected,  U -- Unselected
Local:
Port                    Status  Priority  Key    Flag
--------------------------------------------------------------------------------
GigabitEthernet1/0/2      S       32768     1      {}
GigabitEthernet1/0/3      U       32768     1      {}

Remote:
Actor                   Partner Priority Key   SystemID                Flag
--------------------------------------------------------------------------------
GigabitEthernet1/0/2    0      0        0      0x0000,0000-0000-0000 {}
GigabitEthernet1/0/3    0      0        0      0x0000,0000-0000-0000 {}
```

Table 1-3 Description on the fields of the **display link-aggregation verbose** command

Field	Description
Loadsharing Type	Loadsharing type, including Loadsharing and Non-Loadsharing
Flags	Flag types of LACP
Aggregation ID	Aggregation group ID
Aggregation Description	Aggregation group description string
AggregationType	Aggregation group type
System ID	Device ID
Port Status	Port status, including selected and unselected

display lacp system-id

Syntax

display lacp system-id

View

Any view

Parameters

None

Description

Use the **display lacp system-id** command to display the device ID of the local system, including the system priority and the MAC address.

Examples

Display the device ID of the local system.

```
<Sysname> display lacp system-id
 Actor System ID: 0x8000, 000f-e20f-0100
```

The value of the Actor System ID field is the device ID.

lacp enable

Syntax

lacp enable

undo lacp enable

View

Ethernet port view

Parameters

None

Description

Use the **lacp enable** command to enable LACP on the current port.

Use the **undo lacp enable** command to disable LACP.

By default, LACP is disabled on a port.

Examples

Enable the LACP protocol on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] lacp enable
```

lacp port-priority

Syntax

lacp port-priority *port-priority*

undo lacp port-priority

View

Ethernet port view

Parameters

port-priority: Port priority, ranging from 0 to 65,535.

Description

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

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

By default, the port priority is 32,768.

You can use the **display link-aggregation verbose** command or the **display link-aggregation interface** command to check the configuration result.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] lacp port-priority 64
```

lacp system-priority

Syntax

lacp system-priority *system-priority*

undo lacp system-priority

View

System view

Parameters

system-priority: System priority, ranging from 0 to 65,535.

Description

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

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

By default, the system priority is 32,768.

Examples

Set the system priority to 64.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] lacp system-priority 64
```

link-aggregation group description

Syntax

link-aggregation group *agg-id* **description** *agg-name*

undo link-aggregation group *agg-id* **description**

View

System view

Parameters

agg-id: Aggregation group ID, in the range of 1 to 50.

agg-name: Aggregation group name, a string of 1 to 32 characters.

Description

Use the **link-aggregation group description** command to set a description for an aggregation group.

Use the **undo link-aggregation group description** command to remove the description of an aggregation group.

Note

If you have saved the current configuration with the **save** command, after system reboot, the configuration concerning manual and static aggregation groups and their descriptions still exists, but that of the dynamic aggregation groups and their descriptions gets lost.

You can use the **display link-aggregation verbose** command to check the configuration result.

Examples

Set the description **abc** for aggregation group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] link-aggregation group 1 description abc
```

link-aggregation group mode

Syntax

link-aggregation group *agg-id* **mode** { **manual** | **static** }

undo link-aggregation group *agg-id*

View

System view

Parameters

agg-id: Aggregation group ID, in the range of 1 to 50.

manual: Creates a manual aggregation group.

static: Creates a static aggregation group.

Description

Use the **link-aggregation group mode** command to create a manual or static aggregation group.

Use the **undo link-aggregation group** command to remove the specified aggregation group.

Related commands: **display link-aggregation summary**.

Examples

Create manual aggregation group 22

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] link-aggregation group 22 mode manual
```

port link-aggregation group

Syntax

port link-aggregation group *agg-id*

undo port link-aggregation group

View

Ethernet port view

Parameters

agg-id: Aggregation group ID, in the range of 1 to 50.

Description

Use the **port link-aggregation group** command to add the current Ethernet port to a manual or static aggregation group.

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

Related commands: **display link-aggregation verbose**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 22
```

reset lacp statistics

Syntax

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

View

User view

Parameters

interface-type: Port type

interface-number: Port number

to: Specifies a port index range, with the two *interface-type interface-number* argument pairs around it as the two ends.

Description

Use the **reset lacp statistics** command to clear LACP statistics on specified port(s), or on all ports if no port is specified.

Related commands: **display link-aggregation interface**.

Examples

Clear LACP statistics on all Ethernet ports.

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

Table of Contents

1 Port Isolation Configuration Commands

Port Isolation Configuration Commands

display isolate port

Syntax

display isolate port

View

Any view

Parameters

None

Description

Use the **display isolate port** command to display the Ethernet ports assigned to the isolation group.

Examples

Display the Ethernet ports added to the isolation group.

```
<Sysname> display isolate port
 Isolated port(s) on UNIT 1:
 GigabitEthernet1/0/2, GigabitEthernet1/0/3, GigabitEthernet1/0/4
```

The information above shows that GigabitEthernet1/0/2, GigabitEthernet1/0/3, and GigabitEthernet1/04 are in the isolation group. Neither Layer-2 nor Layer-3 packets can be exchanged between these ports.

port isolate

Syntax

port isolate

undo port isolate

View

Ethernet port view

Parameters

None

Description

Use the **port isolate** command to assign the Ethernet port to the isolation group.

Use the **undo port isolate** command to remove the Ethernet port from the isolation group.

Note

- Assigning or removing an aggregation member port to or from the isolation group can cause the other ports in the aggregation group join or leave the isolation group.
- For ports that belong to an aggregation group and an isolation group simultaneously, removing a port from the aggregation group has no effect on the other ports. That is, the rest ports remain in the aggregation group and the isolation group.
- Ports that belong to an aggregation group and the isolation group simultaneously are still isolated after they are removed from the aggregation group (in system view).
- Assigning an isolated port to an aggregation group causes all the ports in the aggregation group on the local unit to join the isolation group.

By default, the isolation group contains no port.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] port isolate
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] port isolate
```

After the configuration, packets cannot be exchanged between GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

Remove GigabitEthernet 1/0/1 from the isolation group.

```
[Sysname-GigabitEthernet1/0/1] undo port isolate
```

Table of Contents

1 Port Security Commands

Port Security Commands

display mac-address security

Syntax

display mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

Any view

Parameters

Interface *interface-type interface-number*: Specify a port by its type and number, of which the security MAC address information is to be displayed.

vlan *vlan-id*: Specify a VLAN by its ID, of which the security MAC address information is to be displayed. The value range for the *vlan-id* argument is 1 to 4094.

count: Displays the number of matching security MAC addresses.

Description

Use the **display mac-address security** command to display security MAC address entries.

If no argument is specified, the command displays information about all security MAC address entries.

For each security MAC address entry, the output of the command displays the MAC address, the VLAN that the MAC address belongs to, state of the MAC address (which is always security), port associated with the MAC address, and the remaining lifetime of the entry.

By checking the output of this command, you can verify the current configuration.

Examples

Display information about all security MAC address entries.

```
<Sysname> display mac-address security
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
0000-0000-0001  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0002  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0003  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0004  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0001  2         Security       GigabitEthernet1/0/22          NOAGED
0000-0000-0007  2         Security       GigabitEthernet1/0/22          NOAGED

  ---  6 mac address(es) found  ---
```

Display the security MAC address entries for port GigabitEthernet 1/0/20.

```
<Sysname> display mac-address security interface GigabitEthernet 1/0/20
```

```
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
0000-0000-0001  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0002  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0003  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0004  1         Security       GigabitEthernet1/0/20          NOAGED

  ---  4 mac address(es) found on port GigabitEthernet1/0/20 ---
```

Display the security MAC address entries for VLAN 1.

```
<Sysname> display mac-address security vlan 1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
0000-0000-0001  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0002  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0003  1         Security       GigabitEthernet1/0/20          NOAGED
0000-0000-0004  1         Security       GigabitEthernet1/0/20          NOAGED

  ---  4 mac address(es) found in vlan 1 ---
```

Display the total number of security MAC address entries.

```
<Sysname> display mac-address security count
 6 mac address(es) found
```

Display the number of security MAC address entries for VLAN 1.

```
<Sysname> display mac-address security vlan 1 count
 4 mac address(es) found in vlan 1
```

Table 1-1 Description on the fields of the **display mac-address security** command

Field	Description
MAC ADDR	Security MAC address
VLAN ID	VLAN that the MAC address belongs to
STATE	MAC address type, which is always security for a security MAC address
PORT INDEX	Port associated with the MAC address
AGING TIME(s)	Remaining lifetime of the MAC address entry
mac address(es) found	Number of matching security MAC addresses

display port-security

Syntax

display port-security [**interface** *interface-list*]

View

Any view

Parameters

interface *interface-list*: Specify a list of Ethernet ports of which the port security configurations are to be displayed. For the *interface-list* argument, you can specify individual ports and port ranges. An individual port takes the form of *interface-type interface-number* and a port range takes the form of *interface-type interface-number1* **to** *interface-type interface-number2*, with *interface-number2* taking a value greater than *interface-number1*. The total number of individual ports and port ranges defined in the list must not exceed 10.

Description

Use the **display port-security** command to display port security configurations.

If no interface is specified, the command displays the port security configurations of all Ethernet ports.

The output of the command includes the global configurations (such as whether port security is enabled on the switch and whether the sending of specified Trap messages is enabled) and port configurations (such as the security mode and the port security features).

By checking the output of this command, you can verify the current configuration.

Examples

Display the global port security configurations and those of all ports.

```
<Sysname> display port-security
 Equipment port-security is enabled
 AddressLearn trap is Enabled
 Intrusion trap is Enabled
 Dot1x logon trap is Enabled
 Dot1x logoff trap is Enabled
 Dot1x logfailure trap is Enabled
 RALM logon trap is Enabled
 RALM logoff trap is Enabled
 RALM logfailure trap is Enabled
 Disableport Timeout: 20 s
 OUI value:
   Index is 5,  OUI value is 000100
 GigabitEthernet1/0/1 is link-up
   Port mode is AutoLearn
   NeedtoKnow mode is needtoknowonly
   Intrusion mode is BlockMacaddress
   Max mac-address num is 4
   Stored mac-address num is 0
   Authorization is ignore
```

(The rest of the information is omitted.)

Display the port security configurations of ports GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3.

```
<Sysname> display port-security interface GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3
 GigabitEthernet1/0/1 is link-up
   Port mode is AutoLearn
   NeedtoKnow mode is needtoknowonly
   Intrusion mode is BlockMacaddress
```

```
  Max mac-address num is 4
  Stored mac-address num is 0
  Authorization is ignore
GigabitEthernet1/0/2 is link-down
  Port mode is AutoLearn
  NeedtoKnow mode is disabled
  Intrusion mode is no action
  Max mac-address num is not configured
  Stored mac-address num is 0
  Authorization is ignore
GigabitEthernet1/0/3 is link-down
  Port mode is AutoLearn
  NeedtoKnow mode is disabled
  Intrusion mode is BlockMacaddress
  Max mac-address num is not configured
  Stored mac-address num is 0
  Authorization is ignore
```

Table 1-2 Description on the fields of the **display port-security** command

Field	Description
Equipment port security is enabled	Port security is enabled on the switch.
AddressLearn trap is Enabled	The sending of address-learning trap messages is enabled.
Intrusion trap is Enabled	The sending of intrusion-detection trap messages is enabled.
Dot1x logon trap is Enabled	The sending of 802.1x user authentication success trap messages is enabled.
Dot1x logoff trap is Enabled	The sending of 802.1x user logoff trap messages is enabled.
Dot1x logfailure trap is Enabled	The sending of 802.1x user authentication failure trap messages is enabled.
RALM logon trap is Enabled	The sending of MAC-based authentication success trap messages is enabled.
RALM logoff trap is Enabled	The sending of logoff trap messages for MAC-based authenticated users is enabled.
RALM logfailure trap is Enabled	The sending of MAC-based authentication failure trap messages is enabled.
Disableport Timeout: 20 s	The temporary port-disabling time is 20 seconds.
OUI value	The next line displays OUI value.
Index	OUI index
GigabitEthernet1/0/1 is link-up	The link status of port GigabitEthernet 1/0/1 is **up**.
Port mode is AutoLearn	The security mode of the port is **autolearn**.
NeedtoKnow mode is needtoknowonly	The NTK (Need To Know) mode is **ntkonly**.
Intrusion mode is BlockMacaddress	The intrusion detection mode is **BlockMacaddress**.

Field	Description
Max mac-address num is 4	The maximum number of MAC addresses allowed on the port is 4.
Stored mac-address num is 0	No MAC address is stored.
Authorization is ignore	Authorization information delivered by the Remote Authentication Dial-In User Service (RADIUS) server will not be applied to the port.

mac-address security

Syntax

In system view:

mac-address security *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

In Ethernet port view:

mac-address security *mac-address* **vlan** *vlan-id*

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

View

System view, Ethernet port view

Parameters

mac-address: Security MAC address, in the H-H-H format.

interface *interface-type interface-number*: Specify the port on which the security MAC address is to be added. The *interface-type interface-number* arguments indicate the port type and port number.

vlan *vlan-id*: Specify the VLAN to which the MAC address belongs. The *vlan-id* argument specifies a VLAN ID in the range 1 to 4094.

Description

Use the **mac-address security** command to create a security MAC address entry.

Use the **undo mac-address security** command to remove a security MAC address.

By default, no security MAC address entry is configured.

Note

- The **mac-address security** command can be configured successfully only when port security is enabled and the security mode is **autolearn**.
- To create a security MAC address entry successfully, you must make sure that the specified VLAN is carried on the specified port.

Examples

Enable port security; configure the port security mode of GigabitEthernet 1/0/1 as **autolearn** and create a security MAC address entry for 0001-0001-0001, setting the associated port to GigabitEthernet 1/0/1 and assigning the MAC address to VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security enable
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] mac-address security 0001-0001-0001 vlan 1
```

Use the **display mac-address interface** command to verify the configuration result.

```
[Sysname]display mac-address interface GigabitEthernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
0001-0001-0001  1         Security    GigabitEthernet1/0/1            NOAGED

  ---  1 mac address(es) found on port GigabitEthernet1/0/1 ---
```

port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

View

Ethernet port view

Parameters

None

Description

Use the **port-security authorization ignore** command to configure the port to ignore the authorization information delivered by the RADIUS server.

Use the **undo port-security authorization ignore** command to restore the default configuration.

By default, the port uses (does not ignore) the authorization information delivered by the RADIUS server.

You can use the **display port-security** command to check whether the port will use the authorization information delivered by the RADIUS server.

Note

After a RADIUS user passes authentication, the RADIUS server authorizes the attributes configured for the user account such as the dynamic VLAN configuration. For more information, refer to *AAA Command*.

Examples

Configure GigabitEthernet 1/0/2 to ignore the authorization information delivered by the RADIUS server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port-security authorization ignore
```

port-security enable

Syntax

port-security enable

undo port-security enable

View

System view

Parameters

None

Description

Use the **port-security enable** command to enable port security.

Use the **undo port-security enable** command to disable port security.

By default, port security is disabled.

Caution

Enabling port security resets the following configurations on the ports to the defaults (as shown in parentheses below):

- 802.1x (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

Related commands: **display port-security**.

Examples

Enable port security.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security enable
 Notice: The port-control of 802.1x will be restricted to auto when port-security is enabled.
 Please wait... Done.
```

port-security guest-vlan

Syntax

port-security guest-vlan *vlan-id*

undo port-security guest-vlan

View

Ethernet port view

Parameters

vlan-id: Specifies a guest VLAN by its VLAN ID in the range of 1 to 4094. The VLAN must already exist.

Description

Use the **port-security guest-vlan** command to specify an existing VLAN as the guest VLAN of a port.

Use the **undo port-security guest-vlan** command to remove the guest VLAN configuration.

By default, no guest VLAN is specified for a port.

Note that:

- Only an existing VLAN can be specified as a guest VLAN. Make sure the guest VLAN of the port contain the resources that the users need.
- If one user of the port has passed or is undergoing authentication, you cannot specify a guest VLAN for it.
- When a user using a port with a guest VLAN specified fail the authentication, the port is added to the guest VLAN and users of the port can access only the resources in the guest VLAN.
- Multiple users may connect to one port in the **macAddressOrUserLoginSecure** mode for authentication; however, after a guest VLAN is specified, a maximum of one user can pass the security authentication. In this case, the authentication client software of the other 802.1x users displays messages about the failure; MAC address authentication does not have any client software and therefore no such messages will be displayed.
- To change the security mode from **macAddressOrUserLoginSecure** mode of a port that is assigned to a guest VLAN, execute the **undo port-security guest-vlan** command first to remove the guest VLAN configuration.
- For a port configured with both the **port-security guest-vlan** and **port-security intrusion-mode disableport** commands, when authentication of a user fails, only the intrusion detection feature is triggered. The port is not added to the specified guest VLAN.
- It is not recommended to configure the **port-security guest-vlan** and **port-security intrusion-mode blockmac** commands simultaneously for a port. Because when the

authentication of a user fails, the blocking MAC address feature will be triggered and packets of the user will be dropped, making the user unable to access the guest VLAN.

Examples

Set the security mode of port GigabitEthernet 1/0/1 to **macAddressOrUserLoginSecure**, and specify VLAN 100 as the guest VLAN of the port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin-secure-or-mac
[Sysname-GigabitEthernet1/0/1] port-security guest-vlan 100
```

port-security intrusion-mode

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

View

Ethernet port view

Parameters

blockmac: Adds the source MAC addresses of illegal packets to the blocked MAC address list. As a result, the packets sourced from the blocked MAC addresses will be filtered out. A blocked MAC address will be unblocked three minutes (not user configurable) after the block action.

disableport: Disables a port permanently once an illegal frame or event is detected on it.

disableport-temporarily: Disables a port for a specified period of time after an illegal frame or event is detected on it. You can set the period with the **port-security timer disableport** command.

Description

Use the **port-security intrusion-mode** command to set intrusion protection.

Use the **undo port-security intrusion-mode** command to disable intrusion protection.

By default, intrusion protection is not configured.

Note

By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on a port, intrusion protection detects illegal packets (packets with illegal MAC address) or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently and blocking packets with invalid MAC addresses.

The following cases can trigger intrusion protection on a port:

- A packet with unknown source MAC address is received on the port while MAC address learning is disabled on the port.
- A packet with unknown source MAC address is received on the port while the amount of security MAC addresses on the port has reached the preset maximum number.
- The user fails the 802.1x or MAC address authentication.

After executing the **port-security intrusion-mode blockmac** command, you can only use the **display port-security** command to view blocked MAC addresses.

Related commands: **display port-security**, **port-security timer disableport**.

Examples

Configure the intrusion protection mode on GigabitEthernet 1/0/1 as **blockmac**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Display information about blocked MAC addresses after intrusion protection is triggered.

```
<Sysname> display port-security
 Equipment port-security is enabled
 AddressLearn trap is Enabled
 Intrusion trap is Enabled
 Dot1x logon trap is Enabled
 Dot1x logoff trap is Enabled
 Dot1x logfailure trap is Enabled
 RALM logon trap is Enabled
 RALM logoff trap is Enabled
 RALM logfailure trap is Enabled
 Disableport Timeout: 20 s
 OUI value:
   Index is 5,  OUI value is 000100
 Blocked Mac info:
          MAC ADDR             From Port                   Vlan
          --- On unit 1, 2 blocked mac address(es) found. ---
          0000-0000-0003       GigabitEthernet1/0/1             1
          0000-0000-0004       GigabitEthernet1/0/1             1
          --- 2 blocked mac address(es) found. ---
GigabitEthernet1/0/1 is link-up
   Port mode is Secure
```

```
NeedtoKnow mode is disabled
Intrusion mode is BlockMacaddress
Max mac-address num is 2
Stored mac-address num is 2
Authorization is permit
```

For description on the output information, refer to Table 1-2.

Configure the intrusion protection mode on GigabitEthernet 1/0/1 as **disableport-temporarily**. As a result, the port will be disconnected when intrusion protection is triggered and then re-enabled 30 seconds later.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security timer disableport 30
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

Configure the intrusion protection mode on GigabitEthernet 1/0/1 as **disableport**. As a result, when intrusion protection is triggered, the port will be disconnected permanently.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport
```

Note

You can bring up a port that has been permanently disabled by running the **undo shutdown** command or disabling port security on the port.

---

port-security max-mac-count

Syntax

port-security max-mac-count *count-value*

undo port-security max-mac-count

View

Ethernet port view

Parameters

count-value: Maximum number of MAC addresses allowed on the port, in the range of 1 to 1024.

Description

Use the **port-security max-mac-count** command to set the maximum number of MAC addresses allowed on the port.

Use the **undo port-security max-mac-count** command to cancel this limit.

By default, there is no limit on the number of MAC addresses allowed on the port.

Note

By configuring the maximum number of MAC addresses allowed on a port, you can:

- Limit the number of users accessing the network through the port.
- Limit the number of security MAC addresses that can be added on the port.

When the maximum number of MAC addresses allowed on a port is reached, the port will not allow more users to access the network through this port.

Caution

- The **port-security max-mac-count** command is irrelevant to the maximum number of MAC addresses that can be learned on a port configured in MAC address management.
- When there are online users on a port, you cannot perform the **port-security max-mac-count** command on the port.

Examples

Set the maximum number of MAC addresses allowed on the port to 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security enable
[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 { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }

undo port-security ntk-mode

View

Ethernet port view

Parameters

ntkonly: Allows the port to transmit only unicast packets with successfully-authenticated destination MAC addresses.

ntk-withbroadcasts: Allows the port to transmit broadcast packets and unicast packets with successfully-authenticated destination MAC addresses.

ntk-withmulticasts: Allows the port to transmit multicast packets, broadcast packets and unicast packets with successfully-authenticated destination MAC addresses.

Description

Use the **port-security ntk-mode** command to configure the NTK feature on the port.

Use the **undo port-security ntk-mode** command to restore the default setting.

Be default, NTK is disabled on a port, namely all frames are allowed to be sent.

 **Note**

- By checking the destination MAC addresses of the data frames to be sent from a port, the NTK feature ensures that only successfully authenticated devices can obtain data frames from the port, thus preventing illegal devices from intercepting network data.
- Currently, the Switch 4200G Family do not support the **ntkonly** NTK feature.

Examples

Set the NTK feature to **ntk-withbroadcasts** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntk-withbroadcasts
```

port-security oui

Syntax

port-security oui *OUI-value* **index** *index-value*

undo port-security oui index *index-value*

View

System view

Parameters

OUI-value: OUI value. You can input a 48-bit MAC address in the form of H-H-H for this argument and the system will take the first 24 bits as the OUI value and ignore the rest.

index-value: OUI index, ranging from 1 to 16.

 **Note**

The organizationally unique identifiers (OUIs) are assigned by the IEEE to different vendors. Each OUI uniquely identifies an equipment vendor in the world and is the higher 24 bits of a MAC address.

Description

Use the **port-security oui** command to set an OUI value for authentication.

Use the **undo port-security oui** command to cancel the OUI value setting.

By default, no OUI value is set for authentication.

Caution

- The OUI value set by this command takes effect only when the security mode of the port is set to **userLoginWithOUI** by the **port-security port-mode** command.
- The OUI value set by this command cannot be a multicast MAC address.

Related commands: **port-security port-mode**.

Examples

Configure an OUI value of **00ef-ec00-0000**, setting the OUI index to 5.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security oui 00ef-ec00-0000 index 5
```

port-security port-mode

Syntax

port-security port-mode { **autolearn** | **mac-and-userlogin-secure** | **mac-and-userlogin-secure-ext** | **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

Ethernet port view

Parameters

Table 1-3 shows the description on the security mode keywords.

Table 1-3 Keyword description

Keyword	Security mode	Description
autolearn	**autolearn**	In this mode, a port can learn a specified number of MAC addresses and save those addresses as security MAC addresses. It permits only packets whose source MAC addresses are the security MAC addresses that were learned or configured manually. When the number of security MAC addresses reaches the upper limit configured by the **port-security max-count** command, the port changes to work in **secure** mode and no more MAC addresses can be added to the port.
mac-and-userlogin-secure	**macAddressAndUserLoginSecure**	In this mode, users trying to assess the network through the port must first pass MAC address authentication and then 802.1x authentication. In this mode, only one user can access the network through the port at a time.
mac-and-userlogin-secure-ext	**macAddressAndUserLoginSecureExt**	This mode is similar to the **macAddressAndUserLoginSecure** mode, except that in this mode, more than one user can access the network through the port in this mode.
mac-authentication	**macAddressWithRadius**	In this mode, MAC address authentication is applied on users trying to access the network.
mac-else-userlogin-secure	**macAddressElseUserLoginSecure**	In this mode, MAC address authentication is first applied on users. If the authentication succeeds, the users can access the network successfully. If not, 802.1x authentication is applied. In this mode, only one 802.1x-authenticated user can access the network through the port. But at the same time, there can be more than one MAC-address-authenticated user on the port.
mac-else-userlogin-secure-ext	**macAddressElseUserLoginSecureExt**	This mode is similar to the **macAddressElseUserLoginSecure** mode, except that in this mode, there can be more than one 802.1x-authenticated user on the port.
secure	**secure**	In this mode, MAC address learning is disabled on the port. The port permits packets whose source MAC addresses are static and dynamic MAC addresses that were configured manually. When the port mode changes from **autolearn** to **secure**, the security MAC addresses that were learned in the **autolearn** mode are permitted to pass through the port.
userlogin	**userlogin**	In this mode, 802.1x authentication is applied on users trying to access the network through the current port.

Keyword	Security mode	Description
userlogin-secure	**userLoginSecure**	In this mode, MAC-based 802.1x authentication is applied on users trying to access the network through the port. The port will be enabled when the authentication succeeds and allow packets from authenticated users to pass through. In this mode, only one 802.1x-authenticated user can access the network through the port. When the security mode of the port changes from **noRestriction** to this mode, the old dynamic MAC address entries and authenticated MAC address entries kept on the port are deleted automatically.
userlogin-secure-ext	**userLoginSecureExt**	This mode is similar to the **userLoginSecure** mode, except that in this mode, there can be more than one 802.1x-authenticated user on the port.
userlogin-secure-or-mac	**macAddressOrUserLoginSecure**	MAC address authentication and 802.1x authentication can coexist on a port, with 802.1x authentication having higher priority. 802.1x authentication can be applied on users who have already passed MAC address authentication. However, users who have already passed 802.1x authentication do not need to go through MAC address authentication. In this mode, only one 802.1x-authenticated user can access the network through the port. However, there can be more than one MAC-address-authenticated user on the port.
userlogin-secure-or-mac-ext	**macAddressOrUserLoginSecureExt**	This mode is similar to the **macAddressOrUserLoginSecure** mode, except that in this mode, there can be more than one 802.1x-authenticated user on the port.
userlogin-withoui	**userLoginWithOUI**	Similar to the **userLoginSecure** mode, in this mode, there can be only one 802.1x-authenticated user on the port. However, the port also allows packets with the OUI address to pass through. When the security mode of the port changes from **noRestriction** to this mode, the old dynamic MAC address entries and authenticated MAC address entries kept on the port are deleted automatically.

Description

Use the **port-security port-mode** command to set the security mode of the port.

Use the **undo port-security port-mode** command to restore the default mode.

By default, the port is in the **noRestriction** mode, namely access to the port is not restricted.

Note

- Before setting the security mode to **autolearn**, you need to use the **port-security max-mac-count** command to configure the maximum number of MAC addresses allowed on the port.
- When a port operates in the **autolearn** mode, you cannot change the maximum number of MAC addresses allowed on the port.
- After setting the security mode to **autolearn**, you cannot configure static or blackhole MAC addresses on the port.
- When the port security mode is not **noRestriction**, you need to use the **undo port-security port-mode** command to change it back to **noRestriction** before you change the port security mode to other modes.

On a port configured with a security mode, you cannot do the following:

- Configure the maximum number of MAC addresses that can be learned.
- Configure the port as a reflector port for port mirroring.
- Configure link aggregation.

Related commands: **display port-security**.

Examples

Set the security mode of GigabitEthernet 1/0/1 on the switch to **userLogin**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

port-security timer disableport

Syntax

port-security timer disableport *timer*

undo port-security timer disableport

View

System view

Parameters

timer: This argument ranges from 20 to 300, in seconds.

Description

Use the **port-security timer disableport** command to set the time during which the system temporarily disables a port.

Use **undo port-security timer disableport** command restore the default time.

By default, the system disables a port for 20 seconds.

Note

The **port-security timer disableport** command is used in conjunction with the **port-security intrusion-mode disableport-temporarily** command to set the length of time during which the port remains disabled.

Related commands: **port-security intrusion-mode**.

Examples

Set the intrusion protection mode on GigabitEthernet 1/0/1 to **disableport-temporarily**. It is required that when intrusion protection is triggered, the port be shut down temporarily and then go up 30 seconds later.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security timer disableport 30
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

port-security timer guest-vlan-reauth

Syntax

port-security timer guest-vlan-reauth *interval*

undo port-security timer guest-vlan-reauth

View

System view

Parameters

interval: Time period in the range of 1 to 3600, in seconds.

Description

Use the **port-security timer guest-vlan-reauth** command to configure the interval at which the switch triggers MAC address authentication after a port is added to its guest VLAN.

Use the **undo port-security timer guest-vlan-reauth** command to restore the default.

By default, the switch triggers MAC address authentication at intervals of 30 seconds.

At a certain interval, the switch uses the first MAC address learned in the guest VLAN to trigger MAC address authentication. If the authentication succeeds, the port leaves the guest VLAN.

Examples

Configure the switch to trigger MAC address authentication at intervals of 60 seconds.

```
<Sysname> system-view
[Sysname] port-security timer guest-vlan-reauth 60
```

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

Parameters

addresslearned: Enables/disables sending traps for MAC addresses learning events.

dot1xlogfailure: Enables/disables sending traps for 802.1x authentication failures.

dot1xlogoff: Enables/disables sending traps for 802.1x-authenticated user logoff events.

dot1xlogon: Enables/disables sending traps for 802.1x-authenticated user logon events.

intrusion: Enables/disables sending traps for detections of intrusion packets.

ralmlogfailure: Enables/disables sending traps for MAC authentication failures.

ralmlogoff: Enables/disables sending traps for MAC-authenticated user logoff events.

ralmlogon: Enables/disables sending traps for MAC-authenticated user logon events.

 **Note**

RADIUS authenticated login using MAC-address (RALM) refers to MAC-based RADIUS authentication.

Description

Use the **port-security trap** command to enable the sending of specified type(s) of trap messages.

Use the **undo port-security trap** command to disable the sending of specified type(s) of trap messages.

By default, the system disables the sending of any types of trap messages.

 **Note**

This command is based on the device tracking feature, which enables the switch to send trap messages when special data packets (generated by illegal intrusion, abnormal user logon/logoff, or other special activities) are passing through a port, so as to help the network administrator to monitor special activities.

When you use the **display port-security** command to display global information, the system will display which types of trap messages are allowed to send.

Related commands: **display port-security**.

Examples

Allow the sending of intrusion packet-detected trap messages.

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

Use the **display port-security** command to display the related configuration information.

```
<Sysname> display port-security
 Equipment port-security is enabled
 Intrusion trap is Enabled
 Disableport Timeout: 20 s
 OUI value:
 GigabitEthernet1/0/1 is link-down
   Port mode is AutoLearn
   NeedtoKnow mode is needtoknowonly
   Intrusion mode is disableportTemporarily
   Max mac-address num is 4
   Stored mac-address num is 0
   Authorization is ignore
```

The rest of the information is omitted, if any.

For description of the output information, refer to Table 1-2.

2 Port Binding Commands

Port Binding Commands

am user-bind

Syntax

In system view:

am user-bind mac-addr *mac-address* **ip-addr** *ip-address* **interface** *interface-type interface-number*

undo am user-bind mac-addr *mac-address* **ip-addr** *ip-address* **interface** *interface-type interface-number*

In Ethernet port view:

am user-bind mac-addr *mac-address* **ip-addr** *ip-address*

undo am user-bind mac-addr *mac-address* **ip-addr** *ip-address*

View

System view, Ethernet port view

Parameters

interface *interface-type interface-number*: Specify the port to be bound. The *interface-type interface-number* arguments specify the port type and port number.

ip-addr *ip-address*: Specify the IP address to be bound.

mac-addr *mac-address*: Specify the MAC address to be bound. The *mac-address* argument is in the form of H-H-H.

Description

Use the **am user-bind** command to bind the MAC address and IP address of a user to a specified port.

Use the **undo am user-bind** command to cancel the binding.

After the binding, the switch forwards only the packets from the bound MAC address and IP address when received on the port.

By default, no user MAC address or IP address is bound to a port.

Note

- An IP address can be bound with only one port at a time.
- A MAC address can be bound with only one port at a time.

Examples

In system view, bind the MAC address 000f-e200-5101 and IP address 10.153.1.1 (supposing they are MAC and IP addresses of a legal user) to GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] am user-bind mac-addr 000f-e200-5101 ip-addr 10.153.1.1 interface GigabitEthernet1/0/1
```

In Ethernet port view, bind the MAC address 000f-e200-5102 and IP address 10.153.1.2 (supposing they are MAC and IP addresses of a legal user) to GigabitEthernet 1/0/2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] am user-bind mac-addr 000f-e200-5102 ip-addr 10.153.1.2
```

display am user-bind

Syntax

display am user-bind [**interface** *interface-type interface-number* | **ip-addr** *ip-address* | **mac-addr** *mac-address*]

View

Any view

Parameters

interface *interface-type interface-number*: Specify the port to be bound. The *interface-type interface-number* arguments indicate the port type and port number.

ip-addr *ip-address*: Specify the IP address to be bound.

mac-addr *mac-address*: Specify the MAC address to be bound. The *mac-address* argument is in the form of H-H-H.

Description

Use the **display am user-bind** command to display port binding information.

If no keyword is specified, this command displays all port bindings.

Related commands: **am user-bind**.

Examples

Display all port bindings.

```
<Sysname> display am user-bind
Following User address bind have been configured:
  Mac                  IP                   Port
  000f-e200-5101       10.153.1.1           GigabitEthernet1/0/1
  000f-e200-5102       10.153.1.2           GigabitEthernet1/0/2
 Unit 1:Total 2 found, 2 listed.

 Total: 2 found.
```

The above output displays that two port binding settings exist on unit 1:

- MAC address 000f-e200-5101 and IP address 10.153.1.1 are bound to GigabitEthernet 1/0/1.
- MAC address 000f-e200-5102 and IP address 10.153.1.2 are bound to GigabitEthernet 1/0/2.

Table of Contents

1 DLDP Configuration Commands

DLDP Configuration Commands

display dldp

Syntax

display dldp { *unit-id* | *interface-type interface-number* }

View

Any view

Parameters

unit-id: Unit number, only can be set as 1 for S4200G series switch.

interface-type: Port type.

interface-number: Port number.

Description

Use the **display dldp** command to display the DLDP configuration of a unit or a port.

Examples

Display the DLDP configuration of unit 1.

```
<Sysname> display dldp 1
 dldp interval 10
 dldp work-mode enhance
 dldp authentication-mode md5, cipher is ;)<01%^&;YGQ=^Q`MAF4<1!!
 dldp unidirectional-shutdown manual
 dldp delaydown-timer 1

 The port number of unit 1 with DLDP is 1.
interface GigabitEthernet1/0/50
 dldp port state : advertisement
 dldp link state : up
 The neighbor number of the port is 1.
         neighbor mac address : 000f-e20f-7205
         neighbor port index : 372
         neighbor state : two way
         neighbor aged time : 12
```

Table 1-1 Description on the fields of the **display dldp** command

Field	Description
dldp interval	Interval for sending DLDP advertisement packets
dldp work-mode	DLDP work mode
dldp authentication-mode	DLDP authentication mode
cipher	DLDP authentication password
dldp unidirectional-shutdown	DLDP action to be performed on detecting a unidirectional link
dldp delaydown-timer	Setting of the DelayDown timer
The port number of unit 1 with DLDP	Number of the DLDP-enabled ports on unit 1
interface GigabitEthernet1/0/50	Port type and port number
dldp port state	DLDP state of a port
dldp link state	DLDP link state
The neighbor number of the port	Number of the neighbor ports
neighbor mac address	MAC address of a neighbor port
neighbor port index	Neighbor port index
neighbor state	Neighbor state, which can be two way or unknown.
neighbor aged time	Neighbor aging time

dldp

Syntax

dldp { **enable** | **disable** }

View

System view, Ethernet port view

Parameters

None

Description

In system view,

Use the **dldp enable** command to enable DLDP for all the optical ports.

Use the **dldp disable** command to disable DLDP for all the optical ports.

In Ethernet port view,

Use the **dldp enable** command to enable DLDP for the current port.

Use the **dldp disable** command to disable DLDP for the current port.

This command applies to non-optical ports as well as optical ports.

By default, DLDP is disabled.

Caution

When you use the **dldp enable**/**dldp disable** command in system view to enable/disable DLDP on all optical ports of the switch, the configuration takes effect on the existing optical ports, instead of those added subsequently.

Examples

Enable DLDP for all the optical ports of the switch.

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

Enable DLDP on fiber-optic port GigabitEthernet 1/0/50.

```
[Sysname] interface gigabitethernet1/0/50
[Sysname-GigabitEthernet1/0/50] dldp enable
 DLDP is enabled on the port GigabitEthernet1/0/50.
```

dldp authentication-mode

Syntax

dldp authentication-mode { **none** | **simple** *simple-password* | **md5** *md5-password* }

undo dldp authentication-mode

View

System view

Parameters

none: Sets the authentication mode to **none** (Performs no authentication).

simple: Sets the authentication mode to plain text.

simple-password: Authentication password in plain text, a string of 1 to 16 characters.

md5: Sets the authentication mode to MD5.

md5-password: MD5 authentication password, a string in plain text consisting of 1 to 16 characters or a string in cipher text corresponding to the string in plain text.

Description

Use the **dldp authentication-mode** command to set the DLDP authentication mode and password.

Use the **undo dldp authentication-mode** to remove the DLDP authentication mode and password.

By default, the authentication mode is **none**.

Note

- When you configure a DLDP authentication mode and authentication password on a port, make sure that the same DLDP authentication mode and password are set on both the local port and the peer port. Otherwise, DLDP authentication fails.
- DLDP cannot work before DLDP authentication succeeds.

Examples

Set the DLDP authentication mode and password to plain text and **abc** on the ports fiber-connect devices A and B.

- Configure device A

```
<SysnameA> system-view
System View: return to User View with Ctrl+Z.
[SysnameA] dldp authentication-mode simple abc
```

- Configure device B

```
<SysnameB> system-view
System View: return to User View with Ctrl+Z.
[SysnameB] dldp authentication-mode simple abc
```

dldp interval

Syntax

dldp interval *timer-value*

undo dldp interval

View

System view

Parameters

timer-value: Interval for sending DLDP advertisement packets, in the range 1 to 100 (in seconds).

Description

Use the **dldp interval** command to set the interval for sending DLDP advertisement packets for all DLDP-enabled ports in the advertisement state.

Use the **undo dldp interval** command to restore the default.

By default, the interval for sending DLDP advertisement packets is 5 seconds.

Note that:

- The interval takes effect on all the DLDP-enabled ports.
- It is recommended that you set the interval shorter than one-third of the STP convergence time (usually 30 seconds). If too long an interval is set, an STP loop may occur before DLDP shuts down unidirectional links. On the contrary, if too short an interval is set, network traffic increases, unnecessarily consuming port bandwidth.

Examples

Set the interval for sending DLDP advertisement packets to 6 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dldp interval 6
```

dldp reset

Syntax

dldp reset

View

System view, Ethernet port view

Parameters

None

Description

In system view:

Use the **dldp reset** command to reset the DLDP status of all the ports disabled by DLDP.

In Ethernet port view:

Use the **dldp reset** command to reset the DLDP status of the current port disabled by DLDP.

After the **dldp reset** command is executed, the DLDP status of a port changes from **disable** to **active** and DLDP restarts to detect the link status of the fiber cable or copper twisted pair.

Examples

Reset the DLDP status of all the ports disabled by DLDP.

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

dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown

View

System view

Parameters

auto: Disables automatically the corresponding port when DLDP detects an unidirectional link or finds in the enhanced mode that the peer port is down.

manual: Prompts the user to disable manually the corresponding port when DLDP detects an unidirectional link or finds in the enhanced mode that the peer port is down. After the port is disabled, it can only send and receive Recover Probe and Recover Echo packets.

Description

Use the **dldp unidirectional-shutdown** command to set the DLDP handling mode for unidirectional links.

Use the **undo dldp unidirectional-shutdown** command to restore the default DLDP handling mode.

By default, the DLDP handling mode after a unidirectional link is detected is **auto**.

Examples

Configure DLDP to shut down the corresponding port on detecting a unidirectional link.

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

dldp work-mode

Syntax

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode

View

System view

Parameters

enhance: Configures DLDP to work in enhanced mode. In this mode, DLDP detects whether neighbors exist when neighbor tables are aging.

normal: Configures DLDP to work in normal mode. In this mode, DLDP does not detect whether neighbors exist when neighbor tables are aging.

Description

Use the **dldp work-mode** command to set the DLDP operating mode.

Use the **undo dldp work-mode** command to restore the default DLDP operating mode.

By default, DLDP works in normal mode.

Note

- When DLDP works in normal mode, the system can identify only the unidirectional links caused by fiber cross-connection.
- When the DLDP protocol works in enhanced mode, the system can identify two types of unidirectional links: one is caused by fiber cross-connection and the other is caused by one fiber being not connected or being disconnected.

Examples

Configure DLDP to work in enhanced mode.

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

dldp delaydown-timer

Syntax

dldp delaydown-timer *delaydown-time*

undo dldp delaydown-timer

View

System view

Parameters

delaydown-time: Delaydown timer to be set (in seconds). This argument ranges from 1 to 5.

Description

Use the **dldp delaydown-timer** command to set the delaydown timer.

Use the **undo dldp delaydown-timer** command to restore the default delaydown timer setting.

By default, the DelayDown timer is set to 1 second. A period of 5 seconds is recommended.

Note

When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not remove the corresponding neighbor immediately, nor does it transit to the inactive state. Instead, it transits to the delaydown state and starts the DelayDown timer. In delaydown state, the device retains the related DLDP neighbor information. When the DelayDown timer expires, the DLDP neighbor information is removed.

Examples

Set the delaydown timer to 5 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dldp delaydown-timer 5
```

Table of Contents

1 MAC Address Table Management Configuration Commands

Note

This chapter describes the management of static, dynamic, and blackhole MAC address entries. For information about the management of multicast MAC address entries, refer to the “Multicast Protocol” part of the manual.

MAC Address Table Management Configuration Commands

display mac-address aging-time

Syntax

display mac-address aging-time

View

Any view

Parameters

None

Description

Use the **display mac-address aging-time** command to display the aging time of the dynamic MAC address entries in the MAC address table.

Related commands: **mac-address**, **mac-address timer**, **display mac-address**.

Examples

Display the aging time of the dynamic MAC address entries.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The output information indicates that the aging time of the dynamic MAC address entries is 300 seconds.

```
<Sysname> display mac-address aging-time
Mac address aging time: no-aging
```

The output information indicates that dynamic MAC address entries do not age out.

display mac-address

Syntax

display mac-address [*display-option*]

View

Any view

Parameters

display-option: Option used to display specific MAC address table information, as described in Table 1-1.

Table 1-1 Description on the *display-option* argument

Value	Description
mac-address [**vlan** *vlan-id*]	Displays information about a specified MAC address entry.
{ **static** | **dynamic** | **blackhole** } [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	Displays information about dynamic, static, or blackhole MAC address entries.
interface *interface-type interface-number* [**vlan** *vlan-id*] [**count**]	Displays information about the MAC address entries concerning a specified port.
vlan *vlan-id* [**count**]	Displays information about the MAC address entries concerning a specified VLAN.
count	Displays the total number of the MAC address entries maintained by the switch.
statistics	Displays statistics of the MAC address entries maintained by the switch.

mac-address: Specifies a MAC address, in the form of H-H-H.

static: Displays static MAC address entries.

dynamic: Displays dynamic MAC address entries.

blackhole: Displays blackhole MAC address entries.

interface-type interface-number: Specify a port by its interface type and number, of which the MAC address entries are displayed.

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094, in which the MAC address entries are displayed.

count: Displays only the total number of the MAC address entries.

statistics: Displays statistics of the MAC address entries maintained by the switch.

Description

Use the **display mac-address** command to display information about MAC address entries in the MAC address table, including: MAC address, VLAN and port corresponding to the MAC address, the type (static or dynamic) of a MAC address entry, whether a MAC address is within the aging time and so on.

If you specify a unit ID with **unit** *unit-id*, the information about the MAC address entries on the specified device in the fabric will be displayed.

Examples

Display information about MAC address 000f-e20f-0101.

```
<Sysname> display mac-address 000f-e20f-0101
MAC ADDR          VLAN ID   STATE       PORT INDEX            AGING TIME(s)
000f-e20f-0101    1         Learned    GigabitEthernet1/0/1  AGING
```

Display the MAC address entries for the port GigabitEthernet 1/0/4.

```
<Sysname> display mac-address interface GigabitEthernet 1/0/4
MAC ADDR        VLAN ID   STATE       PORT INDEX               AGING TIME(s)
000d-88f6-44ba  1       Learned      GigabitEthernet1/0/4    AGING
000d-88f7-9f7d  1       Learned      GigabitEthernet1/0/4    AGING
000d-88f7-b094  1       Learned      GigabitEthernet1/0/4    AGING
000f-e200-00cc  1       Learned      GigabitEthernet1/0/4    AGING
000f-e200-2201  1       Learned      GigabitEthernet1/0/4    AGING
000f-e207-f2e0  1       Learned      GigabitEthernet1/0/4    AGING
000f-e209-ecf9  1       Learned      GigabitEthernet1/0/4    AGING
---  7 mac address(es) found on port GigabitEthernet1/0/4 ---
```

Display the total number of MAC address entries for VLAN 2.

```
<Sysname> display mac-address vlan 2 count
9 mac address(es) found in vlan 2
```

Table 1-2 Description on the fields of the **display mac-address** command

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs
STATE	The state of the MAC address entry, which can be one of the following: • Config static: Indicates a manually configured static address entry. • Learned: Indicates a dynamically learnt address entry. • Config dynamic: Indicates a manually configured dynamic address entry. • Blackhole: Indicates a blackhole entry.
PORT INDEX	Outgoing port out of which the traffic destined for the MAC address should be sent.
AGING TIME(s)	Indicates whether the MAC address entry is aging. AGING indicates that the entry is aging; NOAGED indicates that the entry will never age out.

mac-address

Syntax

- In system view:

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

undo mac-address [*mac-address-attribute*]

- In Ethernet port view:

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

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

View

System view, Ethernet port view

Parameters

static: Specifies a static MAC address entry.

dynamic: Specifies a dynamic MAC address entry.

blackhole: Specifies a blackhole MAC address entry.

mac-address: Specifies a MAC address, in the form of H-H-H. When entering the MAC address, you can omit the leading 0s in each segment. For example, you can input f-e2-1 for 000f-00e2-0001.

interface-type interface-number: Specifies the outgoing port by its type and number for the MAC address. All traffic destined for the MAC address will be sent out the port.

vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. The VLAN must already exist.

mac-address-attribute: Specifies the criteria for removing MAC address entries. Available syntax options for the argument are described in Table 1-3.

Table 1-3 Available syntax options for the *mac-address-attribute* argument

Syntax	Description
{ **static** | **dynamic** | **blackhole** } **interface** *interface-type interface-number*	Removes the static, dynamic, or blackhole MAC address entries concerning a specified port.
{ **static** | **dynamic** | **blackhole** } **vlan** *vlan-id*	Removes the static, dynamic, or blackhole MAC address entries concerning a specified VLAN.
{ **static** | **dynamic** | **blackhole** } *mac-address* [**interface** *interface-type interface-number*] **vlan** *vlan-id*	Removes a specified static, dynamic, or blackhole MAC address entry.
interface *interface-type interface-number*	Removes all the MAC address entries concerning a specified port.
vlan *vlan-id*	Removes all the MAC address entries concerning a specified VLAN.
mac-address [**interface** *interface-type interface-number*] **vlan** *vlan-id*	Removes a specified MAC address entry.

Description

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

Use the **undo mac-address** command to remove one or more MAC address entries.

In Ethernet port view, the MAC address entry configured with the **mac-address** command in Ethernet port view takes the current Ethernet port as the outgoing port.

If the MAC address you input in the **mac-address** command already exists in the MAC address table, the system will modify the attributes of the corresponding MAC address entry according to your settings in the command.

You can remove all unicast MAC address entries on a port, or remove a specific type of MAC address entries, such as the addresses learnt by the system, dynamic or static MAC address entries configured, or blackhole addresses.

Examples

Configure a static MAC address entry with the following settings:

- MAC address: 000f-e20f-0101
- Outbound port: GigabitEthernet 1/0/1 port
- GigabitEthernet 1/0/1 port belongs to VLAN 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-address static 000f-e20f-0101 interface GigabitEthernet 1/0/1 vlan 2
```

mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

View

Ethernet port view

Parameters

count: Maximum number of MAC addresses a port can learn. This argument ranges from 0 to 4096. A value of 0 disables the port from learning MAC addresses.

Description

Use the **mac-address max-mac-count** command to set the maximum number of MAC addresses an Ethernet port can learn.

Use the **undo mac-address max-mac-count** command to cancel the limitation on the number of MAC addresses an Ethernet port can learn.

By default, the number of MAC addresses an Ethernet port can learn is unlimited.

When you use the **mac-address max-mac-count** command, the port stops learning MAC addresses after the number of MAC addresses it learned reaches the value of the *count* argument you provided. You can use the **undo** command to cancel this limit so that the port can learn MAC addresses without the number limitation. By default, no number limitation is set to the port for MAC address learning.

To prevent illegal devices from accessing the network through a port, you can configure static MAC addresses and disable MAC address learning for the port. Thus, only the packets destined for the configured MAC addresses can be forwarded out the port.

Related commands: **mac-address**, **mac-address timer**.

Examples

Set the maximum number of MAC addresses GigabitEthernet 1/0/3 port can learn to 600.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] mac-address max-mac-count 600
```

mac-address max-mac-count 0

Syntax

mac-address max-mac-count 0

undo mac-address max-mac-count

View

VLAN view

Parameter

None

Description

Use the **mac-address max-mac-count 0** command to disable a switch from learning MAC address in a VLAN.

Use the **undo mac-address max-mac-count** command to enable a switch to learn MAC address in a VLAN.

By default, a switch learns MAC addresses in any VLAN.

Example

Disable the switch from learning MAC address in VLAN 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 3
[Sysname-vlan3] mac-address max-mac-count 0
```

mac-address timer

Syntax

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

undo mac-address timer aging

View

System view

Parameters

aging *age*: Specifies the aging time (in seconds) for dynamic MAC address entries. The *age* argument ranges from 10 to 630.

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

Description

Use the **mac-address timer** command to set the MAC address aging timer.

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

The default MAC address aging timer is 300 seconds.

The timer applies only to dynamic address entries, including both entries learnt and configured.

Setting an appropriate MAC address aging timer is important for the switch to run efficiently.

- If the aging timer is set too short, the MAC address entries that are still valid may be removed. Upon receiving a packet destined for a MAC address that is already removed, the switch broadcasts the packet through all its ports in the VLAN which the packet belongs to. This decreases the operating performance of the switch.
- If the aging timer is set too long, MAC address entries may still exist even if they turn invalid. This causes the switch to be unable to update its MAC address table in time. In this case, the MAC address table cannot reflect the position changes of network devices in time.

Examples

Set the aging time of MAC address entries to 500 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-address timer aging 500
```

Table of Contents

1 MSTP Configuration Commands

MSTP Configuration Commands

active region-configuration

Syntax

active region-configuration

View

MST region view

Parameters

None

Description

Use the **active region-configuration** command to activate the settings of a multiple spanning tree (MST) region.

Configuring MST region-related parameters (especially the VLAN-to-MSTI mapping table) is probable to result in network topology jitter. To reduce network topology jitter caused by the configuration, multiple spanning tree protocol (MSTP) does not recalculate spanning trees immediately after the configuration; it does this only after you activate the new MST region-related settings or enable MSTP, and then the new settings can really take effect.

When you carry out this command, MSTP will replace the currently running MST region–related parameters with the parameters you have just configured and will perform spanning tree recalculation.

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

Examples

Activate the MST region-related settings.

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

bpdu-drop any

Syntax

bpdu-drop any

undo bpdu-drop any

View

Ethernet port view

Parameters

None

Description

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

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

By default, BPDU dropping is disabled.

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

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

Examples

Enable BPDU dropping on GigabitEthernet 1/0/1.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bpdu-drop any
```

check region-configuration

Syntax

check region-configuration

View

MST region view

Parameters

None

Description

Use the **check region-configuration** command to display the MST region-related configuration which is being modified currently, including region name, revision level, and VLAN-to-MSTI mapping table.

As specified in the MSTP protocol, the configurations of MST regions must be right, especially the VLAN-to-MSTI mapping table. MSTP-enabled switches are in the same region only when they have the same format selector (a 802.1s-defined protocol selector, which is 0 by default and cannot be configured), region name, VLAN-to-MSTI mapping table, and revision level. A switch cannot be in the expected region if any of the four MST region-related parameters mentioned above are not consistent with those of another switch in the region.

The 3com switches support only the MST region name, VLAN-to-MSTI mapping table, and revision level. Switches with the settings of these parameters being the same are assigned to the same MST region.

This command is used to display the configuration information of inactivated MST regions. You can use this command to find the MST region the switch currently belongs to or check to see whether or not the MST region-related configuration is correct.

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

Examples

Display the MST region-related configuration.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
   Format selector :0
   Region name     :00e0fc003600
   Revision level  :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 4094
     16       10
```

Table 1-1 Description on the fields of the **check region-configuration** command

Field	Description
Format selector	The selector specified by MSTP
Region name	The name of the MST region
Revision level	The revision level of the MST region
Instance Vlans Mapped	VLAN-to-MSTI mappings in the MST region

display stp

Syntax

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

View

Any view

Parameters

instance-id: ID of the MSTI ranging from 0 to 16. The value of 0 refers to the common and internal spanning tree (CIST).

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

slot *slot-number*: Specifies a slot whose STP-related information is to be displayed.

brief: Displays only port state and protection measures taken on the port.

Description

Use the **display stp** command to display the state and statistical information about one or all spanning trees.

The state and statistical information about MSTP can be used to analyze and maintain the topology of a network. It can also be used to make MSTP operate properly.

- If neither MSTI nor port list is specified, the command displays spanning tree information about all MSTIs on all ports in the order of port number.
- If only one MSTI is specified, the command displays information about the specified MSTI on all ports in the order of the port number.
- If only a port list is specified, the command displays information about all MSTIs on these ports in the order of the port numbers.
- If both an MSTI ID list and a port list are specified, the command displays spanning tree information about the specified MSTIs and the specified ports in the order of MSTI ID.

MSTP state information includes:

1) Global CIST parameters: Protocol operating mode, switch priority in the CIST instance, MAC address, hello time, max age, forward delay, max hops, the common root of the CIST, the external path cost for the switch to reach the CIST common root, region root, the internal path cost for the switch to reach the region root, CIST root port of the switch, the state of the BPDU guard function (enabled or disabled), the state of the digest snooping feature (enabled or disabled), and the state of the TC-BPDU attack guard function (enabled or disabled).
2) CIST port parameters: Port protocol, port role, port priority, path cost, designated bridge, designated port, edge port/non-edge port, whether or not the link on a port is a point-to-point link, format of the MST BPDUs that the port can send, the maximum transmitting speed, type of the enabled guard function, state of the digest snooping feature (enabled or disabled), VLAN mappings, hello time, max age, forward delay, Message-age time, and remaining hops.
3) Global MSTI parameters: MSTI instance ID, bridge priority of the instance, region root, internal path cost, MSTI root port, master bridge, and external path cost..
4) MSTI port parameters: Port state, role, priority, path cost, designated bridge, designated port, remaining hops, and the number of VLANs mapped to the current MSTI.

The statistical information includes: the numbers of the TCN BPDUs, the configuration BPDUs, the RST BPDUs, and the MST BPDUs transmitted/received by each port.

Related commands: **reset stp**.

Examples

Display the brief state information of MSTI 0 on 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
```

Table 1-2 Description on the fields of the **display stp** command

Field	Description
MSTID	ID of an MSTI in the MST region
Port	Port index corresponding to an MSTI
Role	Port role
STP State	STP state on the port, which can be forwarding, discarding, and learning.
Protection	Protection type of the port, which can be one of the following: • ROOT: Root protection • LOOP: Loop protection • BPDU: BPDU protection • NONE: No protection

Display the detailed MSTP status information and statistics information.

```
<Sysname> display stp instance 0 interface GigabitEthernet 1/0/2
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc12-4001
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000f-cb00-6600 / 200
CIST RegRoot/IRPC   :32768.00e0-fc12-4001 / 0
CIST RootPortId     :128.22
BPDU-Protection     :disabled
TC-Protection       :enabled / Threshold=6
Bridge Config
Digest Snooping     :disabled
TC or TCN received  :0
Time since last TC  :0 days 1h:33m:54s

----[Port2(GigabitEthernet1/0/2)][DOWN]----
 Port Protocol       :enabled
 Port Role           :CIST Disabled Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200000
 Desg. Bridge/Port   :32768.00e0-fc12-4001 / 128.2
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=false
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MSTP BPDU format    :Config=auto / Active=legacy
 Port Config
 Digest Snooping     :disabled
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
```

```
BPDU Sent           :0
         TCN: 0, Config: 0, RST: 0, MST: 0
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

Table 1-3 display stp command output description

Field	Description
CIST Bridge	CIST bridge ID
Bridge Times	Major parameters for the bridge: • Hello: Hello timer • MaxAge: Max Age timer • FwDly: Forward delay timer • MaxHop: Max hops within the MST region
CIST Root/ERPC	CIST root and external path cost
CIST RegRoot/IRPC	CIST regional root and internal path cost
CIST RootPortId	CIST root port ID
BPDU-Protection	Indicates whether BPDU protection is enabled globally.
TC-Protection*** / Threshold=**	Indicates whether TC-BPDU attack guard function is enabled globally, and the maximum times that a switch can remove the MAC address table and ARP entries within each 10 seconds.
Bridge Config Digest Snooping	Indicates whether Digest Snooping is enabled globally on the bridge.
TC or TCN received	Number of received TC/TCN packets
Time since last TC	Time of the latest topology change
Port Protocol	Indicates whether STP is enabled on the port
Port Role	Port role, which can be Alternate, Backup, Root, Designated, Master, or Disabled
Port Priority	Port priority
Port Cost(Legacy)	Path cost of the port. The field in the bracket indicates the standard used for port path cost calculation, which can be **legacy**, **dot1d-1998**, or **dot1t**. **Config** indicates the configured value, and **Active** indicates the actual value.
Desg. Bridge/Port	Designated bridge ID and port ID of the port The port ID displayed is insignificant for a port which does not support port priority.
Port Edged	Indicates whether the port is an edge port. **Config** indicates the configured value, and **Active** indicates the actual value.
Point-to-point	Indicates whether the port is connected to a point-to-point link. **Config** indicates the configured value, and **Active** indicates the actual value.
Transmit Limit	The maximum number of packets sent within each Hello time
Protection Type	Protection type on the port, including Root guard and Loop guard
MST BPDU format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s. **Config** indicates the configured value, and **Active** indicates the actual value.

Field	Description
Port Config Digest Snooping	Indicates whether digest snooping is enabled on the port.
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI
PortTimes	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

display stp abnormalport

Syntax

display stp abnormalport

View

Any view

Parameters

None

Description

Use the **display stp abnormalport** command to display the ports that are blocked by STP guard functions.

Examples

Display the ports that are blocked by STP guard functions.

```
<Sysname> display stp abnormalport
MSTID        Port                    Block Reason
-------- --------------------    -------------
  0          GigabitEthernet1/0/20   Root-Protection
  1          GigabitEthernet1/0/21   Loop-Protection
```

Table 1-4 Description on the fields of the **display stp abnormalport** command

Field	Description
MSTID	MSTI ID in the MST region
Port	Port that has been blocked
Block Reason	The function blocking the port

display stp portdown

Syntax

display stp portdown

View

Any view

Parameters

None

Description

Use the **display stp portdown** command to display the ports that are shut down by STP guard functions.

Examples

Display the ports that are shut down by STP guard functions.

```
<Sysname> display stp portdown
Port                   Down Reason
---------------------  ------------
GigabitEthernet1/0/20  BPDU-Protection
```

Table 1-5 Description on the fields of the **display stp portdown** command

Field	Description
Port	Port that has been shut down
Down Reason	The function shutting down the port

display stp region-configuration

Syntax

display stp region-configuration

View

Any view

Parameters

None

Description

Use the **display stp region-configuration** command to display the activated MST region configuration, including the region name, region revision level, and VLAN-to-STI mappings configured for the switch.

Related commands: **stp region-configuration**.

Examples

Display the configuration of the MST region.

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

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

Table 1-6 Description on the fields of the **display stp region-configuration** command

Field	Description
Format selector	The selector specified by MSTP
Region name	The name of the MST region
Revision level	The revision level of the MST region
Instance Vlans Mapped	VLAN-to-STI mappings in the MST region

display stp root

Syntax

display stp root

View

Any view

Parameters

None

Description

Use the **display stp root** command to display information about the root ports in the MSTP region where the switch resides.

Examples

Display information about the root ports in the MSTP region where the switch resides.

```
<Sysname> display stp root
  MSTID Root Bridge ID       ExtPathCost IntPathCost Root Port
--------  ------------------- ------------  ------------- -----------
  0     32768.00e0-fc53-d908  0             200           GigabitEthernet1/0/18
```

Table 1-7 Description on the fields of the **display stp root** command

Field	Description
MSTID	MSTI ID in the MST region
Root Bridge ID	ID of the root bridge

Field	Description
ExtPathCost	Cost of the external path from the switch to the root bridge
IntPathCost	Cost of the internal path from the switch to the root bridge
Root Port	Root port (If a port on the current device is an MSTI root port, the port type and port number is displayed. Otherwise, the root port name is not displayed.)

instance

Syntax

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

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

View

MST region view

Parameters

instance-id: ID of an MSTI ranging from 0 to 16. The value of 0 refers to the CIST.

vlan-list: List of VLANs. You need to provide this argument in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where &<1-10> means that you can provide up to 10 VLAN IDs/VLAN ID ranges for this argument. Normally, a VLAN ID can be a number ranging from 1 to 4094.

Description

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

Use the **undo instance** command to remove the mappings from the specified VLANs to the specified MSTI and remap the specified VLANs to the CIST (MSTI 0). If you specify no VLAN in the **undo instance** command, all VLANs that are mapped to the specified MSTI are remapped to the CIST.

By default, all VLANs are mapped to the CIST.

VLAN-to-MSTI mappings are recorded in the VLAN-to-MSTI mapping table of an MSTP-enabled switch. So these two commands are actually used to manipulate the VLAN-to-MSTI mapping table. You can add/remove a VLAN to/from the VLAN-to-MSTI mapping table of a specific MSTI by using these two commands.

Note that a VLAN cannot be mapped to multiple MSTIs at the same time. A VLAN-to-MSTI mapping is automatically removed if you map the VLAN to another MSTI.

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

Examples

Map VLAN 2 to MSTI 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

region-name

Syntax

region-name *name*

undo region-name

View

MST region view

Parameters

name: MST region name to be set for the switch, a string of 1 to 32 characters.

Description

Use the **region-name** command to set an MST region name for a switch.

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

The default MST region name of a switch is its MAC address.

MST region name, along with VLAN-to-MSTI mapping table and MSTP revision level, determines the MST region which a switch belongs to.

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

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

reset stp

Syntax

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

View

User view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **reset stp** command to clear spanning tree statistics.

The spanning tree statistics includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs, and MST BPDUs sent/received through one or more specified ports or all ports (note that BPDUs and TCN BPDUs are counted only for CISTs.)

Note that:

- If you specify the *interface-list* argument, this command clears the spanning tree statistics on specified ports.
- If you do not specify the *interface-list* argument, this command clears the spanning tree statistics on all ports.

Related commands: **display stp**.

Examples

Clear the spanning tree statistics on 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

Parameters

level: MSTP revision level to be set for the switch. This argument ranges from 0 to 65,535.

Description

Use the **revision-level** command to set the MSTP revision level for a switch.

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

By default, the MSTP revision level of a switch is 0.

MSTP revision level, along with MST region name and VLAN-to-MSTI mapping table, determines the MST region which a switch belongs to.

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

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

stp

Syntax

stp { **enable** | **disable** }

undo stp

View

System view, Ethernet port view

Parameters

enable: Enables MSTP globally or on a port.

disable: Disables MSTP globally or on a port.

Description

Use the **stp** command to enable/disable MSTP globally or on a port.

Use the **undo stp** command to restore the MSTP state to the default globally or on a port.

By default, MSTP is enabled both globally and on a port.

After MSTP is enabled, the actual operating mode, which can be STP-compatible mode, RSTP-compatible mode, or MSTP mode, is determined by the user-defined protocol mode. A switch becomes a transparent bridge if MSTP is disabled.

After being enabled, MSTP maintains spanning trees by processing configuration BPDUs of different VLANs. After being disabled, it stops maintaining spanning trees.

Related commands: **stp mode**, **stp interface**.

Examples

Enable MSTP globally.

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

Disable MSTP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp disable
```

stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

View

System view

Parameters

None

Description

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

Use the **undo stp bpdu-protection** command to restore to the default state of the BPDU guard function.

By default, the BPDU guard function is disabled.

Normally, the access ports of the devices operating on the access layer are directly connected to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to implement rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning trees recalculation and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent such attacks by enabling the BPDU guard function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. If an edge port is shut down, only the administrator can restore it.

Examples

Enable the BPDU guard function.

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

stp bridge-diameter

Syntax

stp bridge-diameter *bridgenum*

undo stp bridge-diameter

View

System view

Parameters

bridgenum: Network diameter to be set for a switched network. This argument ranges from 2 to 7.

Description

Use the **stp bridge-diameter** command to set the network diameter of a switched network. The network diameter of a switched network is represented by the maximum possible number of switches between any two terminal devices in a switched network.

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

By default, the network diameter is 7.

After you configure the network diameter of a switched network, MSTP adjusts its hello time, forward delay, and max age settings accordingly. With the network diameter set to the default value 7, the three time-relate settings, including hello time, forward delay, and max age, are set to their default values as well.

The **stp bridge-diameter** command only applies to CIST. It is invalid for MSTIs.

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

Examples

Set the network diameter to 5.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp bridge-diameter 5
```

stp compliance

Syntax

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

undo stp compliance

View

Ethernet port view

Parameters

auto: Specifies the port to recognize and send MSTP packets in the automatic mode.

legacy: Specifies the port to recognize and send MSTP packets in the legacy mode.

dot1s: Specifies the port to recognize and send MSTP packets in the 802.1s mode.

Description

Use the **stp compliance** command to set the mode in which a port recognizes and sends MSTP packets.

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

By default, a port recognizes and sends MSTP packets in the automatic mode.

A port can be configured to recognize and send MSTP packets in the following modes.

- Automatic mode. Ports in this mode determine the format of the MSTP packets to be sent according to the format of the received packets.
- Legacy mode. Ports in this mode recognize/send packets in legacy format.
- 802.1s mode. Ports in this mode recognize/send packets in dot1s format.

A port acts as follows according to the format of MSTP packets forwarded by a peer switch or router.

When a port operates in the automatic mode:

- The port automatically determines the format (legacy or dot1s) of received MSTP packets and then determines the format of the packets to be sent accordingly, thus communicating with the peer devices.
- If the format of the received packets changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be brought up again by the network administrator.

When a port operates in the legacy mode:

- The port only recognizes and sends MSTP packets in legacy format. In this case, the port can only communicate with the peer through packets in legacy format.
- If packets in dot1s format are received, the port turns to discarding state to prevent network storm.

When a port operates in the 802.1s mode:

- The port only recognizes and sends MSTP packets in dot1s format. In this case, the port can only communicate with the peer through packets in dot1s format.
- If packets in legacy format are received, the port turns to discarding state to prevent network storm.

Examples

Configure GigabitEthernet 1/0/1 to recognize and send MSTP packets in dot1s format.

```
<Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

Restore the default mode in which a port recognizes and send MSTP packets.

```
[Sysname-GigabitEthernet1/0/1] undo stp compliance
```

stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

View

System view, Ethernet port view

Parameters

None

Description

Use the **stp config-digest-snooping** command to enable the digest snooping feature globally.

Use the **undo stp config-digest-snooping** command to disable the digest snooping feature globally.

The digest snooping feature is disabled by default.

According to IEEE 802.1s, two interconnected switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. With MSTP enabled, interconnected switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some other manufacturers' switches adopt proprietary spanning tree protocols, they cannot interwork with other switches in an MST region even if they are configured with the same MST region-related settings as other switches in the MST region.

This kind of problems can be overcome by implementing the digest snooping feature. If a switch port is connected to another manufacturer’s switch that has the same MST region-related settings but adopts a proprietary spanning tree protocol, you can enable the digest snooping feature on the port when it receives BPDU packets from another manufacturer's switch. Then the switch considers these BPDU packets to be from its own MST region and records the configuration digests carried in the BPDU packets received from the switch, which will be put in the BPDU packets to be sent to another manufacturer’s switch. In this way, the switch can interwork with another manufacturer’s switches in an MST region.

Note

- When the digest snooping feature is enabled on a port, the port turns to the discarding state. That is, the port stops sending BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.
- The digest snooping feature is needed only when your switch is connected to another manufacturer's switches adopting proprietary spanning tree protocols.
- To enable the digest snooping feature successfully, you must first enable it on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols and then enable it globally.
- To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).
- The digest snooping feature must be enabled on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols in the same MST region.
- When the digest snooping feature is enabled globally, the VLAN-to-MSTI mapping table cannot be modified.
- The digest snooping feature is not applicable to boundary ports in an MST region.
- The digest snooping function is not applicable to edge ports in an MST region.

Examples

Enable the digest snooping feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp config-digest-snooping
```

stp cost

Syntax

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

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

View

Ethernet port view

Parameters

instance-id: ID of an MSTI ranging from 0 to 16. The value of 0 refers to the CIST.

cost: Path cost to be set for the port. The range of the *cost* argument varies with the standard used for calculating the default path cost of a port as follows:

- With the IEEE 802.1D-1998 standard selected, the path cost of an Ethernet port ranges from 1 to 65535.
- With the IEEE 802.1t standard selected, the path cost of an Ethernet port ranges from 1 to 200000000.
- With the proprietary standard selected, the path cost of an Ethernet port ranges from 1 to 200000.

Description

Use the **stp cost** command to set the path cost of the current port in a specified MSTI.

Use the **undo stp cost** command to restore the default path cost of the current port in the specified MSTI.

By default, a switch automatically calculates the path costs of a port in different MSTIs based on a specified standard.

If you specify the *instance-id* argument to be 0 or do not specify this argument, the **stp cost** command sets the path cost of the port in CIST.

The path cost of a port affects its port role. By configuring different path costs for the same port in different MSTIs, you can make flows of different VLANs travel along different physical links, so as to achieve VLAN-based load balancing. Changing the path cost of a port in an MSTI may change the role of the port in the instance and put it in state transition.

Related commands: **stp interface cost**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 cost 200
```

stp dot1d-trap

Syntax

stp dot1d-[**instance** *instance-id*] **trap** [**newroot** | **topologychange**] **enable**

undo stp [**instance** *instance-id*] **dot1d-trap** [**newroot** | **topologychange**] **enable**

View

System view

Parameters

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to CIST. With this argument specified, the trap messages sent are only of the MSTI identified by this argument.

newroot: Sends trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of an instance.

topologychange: Sends trap messages conforming to 802.1d standard to the network management device when the switch detects network topology changes.

Description

Use the **stp dot1d-trap** command to enable a switch to send trap messages conforming to 802.1d standard when MSTP network topology changes.

Use the **undo stp dot1d-trap** command to disable this function.

A switch sends trap messages conforming to 802.1d standard to the network management device when:

- The switch becomes the root bridge of an MSTI.
- Network topology changes are detected.

Examples

Enable a switch to send trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of MSTI 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp instance 1 dot1d-trap newroot enable
```

stp edged-port

Syntax

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

undo stp edged-port

View

Ethernet port view

Parameters

enable: Configures the current Ethernet port as an edge port.

disable: Configures the current Ethernet port as a non-edge port.

Description

Use the **stp edged-port enable** command to configure the current Ethernet port as an edge port.

Use the **stp edged-port disable** command to configure the current Ethernet port as a non-edge port.

Use the **undo stp edged-port** command to restore the current Ethernet port to its default state.

By default, all Ethernet ports of a switch are non-edge ports.

An edge port is a port that is directly connected to a user terminal instead of another switch or shared network segment. Rapid transition to the forwarding state is applied to edge ports because on these ports no loops can be incurred by network topology changes. You can enable a port to turn to the forwarding state rapidly by setting it to an edge port. And you are recommended to configure the Ethernet ports directly connected to user terminals as edge ports to enable them to turn to the forwarding state rapidly.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But when the BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it turns to a non-edge port.

Related commands: **stp interface edged-port**.

Caution

With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

Examples

Configure GigabitEthernet 1/0/1 as a non-edge port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port disable
```

stp interface

Syntax

stp interface *interface-list* { **enable** | **disable** }

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

enable: Enables MSTP on the specified ports.

disable: Disables MSTP on the specified ports.

Description

Use the **stp interface** command to enable or disable MSTP on specified ports in system view.

By default, MSTP is enabled on the ports of a switch if MSTP is globally enabled on the switch, and MSTP is disabled on the ports if MSTP is globally disabled.

An MSTP-disabled port does not participate in any spanning tree calculation and is always in the forwarding state.

Caution

Disabling MSTP on ports may result in loops.

Related commands: **stp mode**, **stp**.

Examples

Enable MSTP on GigabitEthernet 1/0/1 in system view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/1 enable
```

stp interface compliance

Syntax

stp interface *interface-list* **compliance** { **auto** | **legacy** | **dot1s** }

undo stp interface *interface-list* **compliance**

View

System view

Parameter

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the format of *interface-list* ={ *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

auto: Specifies the port to recognize and send MSTP packets in the automatic mode.

legacy: Specifies the port to recognize and send MSTP packets in the legacy mode.

dot1s: Specifies the port to recognize and send MSTP packets in the 802.1s mode.

Description

Use the **stp interface compliance** command to set the mode in which a port recognizes and sends MSTP packets.

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

By default, a port recognizes and sends MSTP packets in the automatic mode.

A port can be configured to recognize and send MSTP packets in the following modes.

- Automatic mode. Ports in this mode determine the format of the MSTP packets to be sent according to the format of the received packets.
- Legacy mode. Ports in this mode recognize/send packets in legacy format.
- 802.1s mode. Ports in this mode recognize/send packets in dot1s format.

A port acts as follows according to the format of MSTP packets forwarded by a peer switch or router.

When a port operates in the automatic mode:

- The port automatically determines the format (legacy or dot1s) of received MSTP packets and then determines the format of the packets to be sent accordingly, thus communicating with the peer devices.
- If the format of the received packets changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be brought up again by the network administrator.

When a port operates in the legacy mode:

- The port only recognizes and sends MSTP packets in legacy format. In this case, the port can only communicate with the peer through packets in legacy format.
- If packets in dot1s format are received, the port turns to discarding state to prevent network storm.

When a port operates in the 802.1s mode:

- The port only recognizes and sends MSTP packets in dot1s format. In this case, the port can only communicate with the peer through packets in dot1s format.
- If packets in legacy format are received, the port turns to discarding state to prevent network storm.

Example

Configure GigabitEthernet 1/0/1 to recognize and send MSTP packets in dot1s format.

```
<Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[Sysname] stp interface GigabitEthernet1/0/1 compliance dot1s
```

Restore the default mode in which a port recognizes and send MSTP packets.

```
[Sysname] undo stp interface GigabitEthernet1/0/1 compliance
```

stp interface config-digest-snooping

Syntax

stp interface *interface-list* **config-digest-snooping**

undo stp interface *interface-list* **config-digest-snooping**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the format of *interface-list* ={ *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **stp interface config-digest-snooping** command to enable the digest snooping feature on specific ports.

Use the **undo stp interface config-digest-snooping** command to disable the digest snooping feature on specific ports.

By default, the digest snooping feature is disabled on a port.

According to IEEE 802.1s, two interconnected MSTP switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some another manufacturer’s switches adopt proprietary spanning tree protocols, they cannot interwork with other switches in an MST region even if they are configured with the same MST region-related settings as other switches in the MST region.

This kind of problems can be overcome by implementing the digest snooping feature. If a switch port is connected to another manufacturer's switch that has the same MST region-related settings but adopts a proprietary spanning tree protocol, you can enable the digest snooping feature on the port when it receives BPDU packets from another manufacturer's switch. Then the switch considers these BPDU packets to be from its own MST region and records the configuration digests carried in the BPDU packets received from the switch, which will be put in the BPDU packets to be sent to the another manufacturer's switch. In this way, the switch can interwork with another manufacturer's switches in an MST region.

Note

- When the digest snooping feature is enabled on a port, the port turns to the discarding state. That is, the port stops sending BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.
- The digest snooping feature is needed only when your switch is connected to another manufacturer's switches adopting proprietary spanning tree protocols.
- To enable the digest snooping feature successfully, you must first enable it on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols and then enable it globally.
- To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).
- The digest snooping feature must be enabled on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols in the same MST region.
- When the digest snooping feature is enabled globally, the VLAN-to-MSTI mapping table cannot be modified.
- The digest snooping feature is not applicable to boundary ports in an MST region.
- The digest snooping function is not applicable to edge ports in an MST region.

Examples

Enable the digest snooping feature for GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/1 config-digest-snooping
```

stp interface cost

Syntax

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

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

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

cost: Path cost to be set for the port. The range of the *cost* argument varies with the standard used for calculating the default path cost of a port as follows:

- With the IEEE 802.1D-1998 standard selected, the path cost of an Ethernet port ranges from 1 to 65535.
- With the IEEE 802.1t standard selected, the path cost of an Ethernet port ranges from 1 to 200000000.
- With the proprietary standard selected, the path cost of an Ethernet port ranges from 1 to 200000.

Description

Use the **stp interface cost** command to set the path cost(s) of the specified port(s) in a specified MSTI in system view.

Use the **undo stp interface cost** command to restore the default value of the path cost(s) of the specified port(s) in the specified MSTI in system view.

By default, a switch automatically calculates the path costs of a port in different MSTIs based on a specified standard.

If you specify the *instance-id* argument to be 0 or do not specify this argument, the **stp interface cost** command sets the path cost(s) of the specified port(s) in the CIST.

The path cost of a port affects its port role. By configuring different path costs for the same port in different MSTIs, you can make flows of different VLANs travel along different physical links, so as to achieve VLAN-based load balancing. Changing the path cost of a port in an MSTI may change the role of the port in the instance and put it in state transition.

The default port path cost varies with port speed. Refer to Table 1-8 for details.

Related commands: **stp cost**.

Examples

Set the path cost of GigabitEthernet 1/0/3 in MSTI 2 to 400.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 instance 2 cost 400
```

stp interface edged-port

Syntax

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

undo stp interface *interface-list* **edged-port**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

enable: Configures the specified Ethernet port to be an edge port.

disable: Configures the specified Ethernet port to be a non-edge port.

Description

Use the **stp interface edged-port enable** command to configure the specified Ethernet ports as edge ports in system view.

Use the **stp interface edged-port disable** command to configure the specified Ethernet ports as non-edge ports in system view.

Use the **undo stp interface edged-port** command to restore the specified Ethernet ports to the default state.

By default, all Ethernet ports of a switch are non-edge ports.

An edge port is a port that is directly connected to a user terminal instead of another switch or a network segment. Rapid transition to the forwarding state is applied to edge ports because on these ports no loops can be incurred by network topology changes. You can enable a port to turn to the forwarding state rapidly by setting it to an edge port. And you are recommended to configure the Ethernet ports directly connected to user terminals as edge ports to enable them to turn to the forwarding state rapidly.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But when the BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it turns to a non-edge port.

Related commands: **stp edged-port**.

Caution

With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

Examples

Configure GigabitEthernet 1/0/3 as an edge port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 edged-port enable
```

stp interface loop-protection

Syntax

stp interface *interface-list* **loop-protection**

undo stp interface *interface-list* **loop-protection**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **stp interface loop-protection** command to enable the loop guard function in system view.

Use the **undo stp interface loop-protection** command to restore the default state of the loop guard function in system view.

The loop guard function is disabled by default.

Related commands: **stp loop-protection**.

Caution

With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/1 loop-protection
```

stp interface mcheck

Syntax

stp [**interface** *interface-list*] **mcheck**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **stp interface mcheck** command to perform the mCheck operation on specified port(s) in system view.

A port on an MSTP-enabled switch migrates to the STP-/RSTP-compatible mode automatically if an STP-/RSTP-enabled switch has been connected to it. But when the STP-/RSTP-enabled switch is disconnected from the port, the port cannot migrate back to the MSTP mode automatically. In this case, you can force the port to migrate to the MSTP mode by performing the mCheck operation on the port.

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

Examples

Perform the mCheck operation for GigabitEthernet 1/0/3 in system view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 mcheck
```

stp interface no-agreement-check

Syntax

stp interface *interface-type interface-number* **no-agreement-check**

undo stp interface *interface-type interface-number* **no-agreement-check**

View

System view

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **stp interface no-agreement-check** command to enable the rapid transition feature on the specified port.

Use the **undo stp interface no-agreement-check** command to disable the rapid transition feature on the specified port.

The rapid transition feature is disabled on any port by default.

Some manufactures' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operates as the upstream switch of the 3com switches running MSTP, the upstream designated port fails to change their states rapidly.

The rapid transition feature is developed on the 3com switches to avoid this case. When a 3com switch running MSTP is connected in the upstream direction to a manufacture's switch adopting proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the 3com switch operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Related commands: **stp no-agreement-check**.

Note

- The rapid transition feature can be enabled on root ports or alternate ports only.
- You can enable the rapid transition feature on the designated port, however, the feature does not take effect on the port.

Examples

Enable the rapid transition feature for GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]stp interface GigabitEthernet 1/0/1 no-agreement-check
```

stp interface point-to-point

Syntax

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

undo stp interface *interface-list* **point-to-point**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

force-true: Specifies that the links connected to the specified Ethernet ports are point-to-point links.

force-false: Specifies that the links connected to the specified Ethernet ports are not point-to-point links.

auto: Specifies to automatically determine whether or not the links connected to the specified Ethernet ports are point-to-point links.

Description

Use the **stp interface point-to-point** command to specify whether the links connected to the specified Ethernet ports are point-to-point links in system view.

Use the **undo stp interface point-to-point** command to restore the links connected to the specified ports to their default link types, which are automatically determined by MSTP.

If no keyword is specified in the **stp interface point-to-point** command, the **auto** keyword is used by default, and so MSTP automatically determines the types of the links connected to the specified ports.

The rapid transition feature is not applicable to ports connected to non-point-to-point links.

If an Ethernet port is the master port of aggregated ports or operates in full-duplex mode, the link connected to the port is a point-to-point link. You are recommended to let MSTP automatically determine the link types.

These two commands apply to CIST and MSTIs. If you configure the link to which a port is connected to be a point-to-point link (or a non-point-to-point link), the configuration applies to all MSTIs (that is, the port is configured to connect to a point-to-point link (or a non-point-to-point link) in all MSTIs). If the actual physical link is not a point-to-point link and you configure the link to which the port is connected to be a point-to-point link, loops may temporarily occur.

Related commands: **stp point-to-point**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 point-to-point force-true
```

stp interface port priority

Syntax

stp interface *interface-list* **instance** *instance-id* **port priority** *priority*

undo stp interface *interface-list* **instance** *instance-id* **port priority**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

priority: Port priority to be set. This argument ranges from 0 to 240 and must be a multiple of 16 (such as 0, 16, 32, and so on).

Description

Use the **stp interface port priority** command to set a port priority for the specified ports in the specified MSTI in system view.

Use the **undo stp interface port priority** command to restore the default priority of the specified ports in the specified MSTI in system view.

The default port priority of a port in an MSTI is 128.

If you specify the *instance-id* argument to 0, the two commands apply to the port priorities on the CIST. The role a port plays in an MSTI is affected by its port priority in the instance. A port on an MSTP-enabled switch can have different port priorities and play different roles in different MSTIs. This enables packets of different VLANs to be forwarded along different physical paths, so as to implement VLAN-based load balancing. Changing port priorities results in port role recalculation and may cause state transition.

Related commands: **stp port priority**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 instance 2 port priority 16
```

stp interface root-protection

Syntax

stp interface *interface-list* **root-protection**

undo stp interface *interface-list* **root-protection**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **stp interface root-protection** command to enable the root guard function on specified port(s) in system view.

Use the **undo stp interface root-protection** command to restore the root guard function to the default state on specified port(s) in system view.

By default, the root guard function is disabled.

Because of configuration errors or malicious attacks, the root bridge in the network may receive configuration BPDUs with priorities higher than that of a root bridge, which causes new root bridge to be elected and network topology jitter to occur. In this case, flows that should have traveled along high-speed links are led to low-speed links, which causes network congestion.

You can avoid this problem by enabling the root guard function. Root-guard-enabled ports can only be kept as designated ports in all MSTIs. When a port of this type receives configuration BPDUs with higher priorities, that is, when it is to become a non-designated port, it turns to the discarding state and stops forwarding packets (as if it is disconnected from the link).

Related commands: **stp root-protection**.

Caution

With the loop guard function enabled, the root guard function and edge port configuration are mutually exclusive.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/1 root-protection
```

stp interface transmit-limit

Syntax

stp interface *interface-list* **transmit-limit** *packetnum*

undo stp interface *interface-list* **transmit-limit**

View

System view

Parameters

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

packetnum: Maximum number of configuration BPDUs a port can send in each hello time. This argument ranges from 1 to 255 and defaults to 10.

Description

Use the **stp interface transmit-limit** command to set the maximum number of configuration BPDUs each specified port can send in each hello time.

Use the **undo stp interface transmit-limit** command to restore the maximum number to the default value.

The larger the *packetnum* argument is, the more packets a port can transmit in each hello time, while the more switch resources are occupied. Configure the *packetnum* argument to a proper value to limit the number of BPDUs a port can send in each hello time to prevent MSTP from occupying too much bandwidth resources when network topology jitter occur.

Related commands: **stp transmit-limit**.

Examples

Set the maximum transmitting speed of GigabitEthernet 1/0/3 to 15.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp interface GigabitEthernet 1/0/3 transmit-limit 15
```

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

Ethernet port view

Parameters

None

Description

Use the **stp loop-protection** command to enable the loop guard function on the current port.

Use the **undo stp loop-protection** command to restore the loop guard function to the default state on the current port.

By default, the loop guard function is disabled.

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestion or unidirectional link failures. If a switch does not receive BPDUs from the upstream switch for a certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports turn to the forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or unidirectional link failures happen, a root port becomes a designated port, and the port turns to the discarding state. The blocked port also becomes the designated port and the port turns to the discarding state, that is, the port does not forward packets and thereby loops can be prevented.

Examples

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

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

Parameters

hops: Maximum hop count to be set. This argument ranges from 1 to 40.

Description

Use the **stp max-hops** command to set the maximum hop count for the MST region the current switch belongs to.

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

By default, the maximum hop count of an MST region is 20.

The maximum hop count configured on the region roots of an MST region limits the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in a MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes one switch. Such a mechanism disables the switches that are beyond the maximum hops from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hops configured on the switch operating as the root bridge of the CIST or an MSTI in a MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in an MST region adopt the maximum hop settings of the root bridge.

Examples

Set the maximum hop count of the current MST region to 35.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp max-hops 35
```

stp mcheck

Syntax

stp mcheck

View

System view, Ethernet port view

Parameters

None

Description

Use the **stp mcheck** command to perform the mCheck operation on the current port.

When a port on an MSTP-enabled upstream switch connects with an STP-enabled downstream switch, the port operates in the STP-compatible mode automatically. But when the STP-enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode but still remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, when a port on an RSTP-enabled upstream switch connects with an STP-enabled downstream switch, the port operates in the STP-compatible mode. But when the STP-enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode but remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP-compatible mode by performing the mCheck operation on the port.

Related commands: **stp mode**, **stp interface mcheck**.

Examples

Perform the mCheck operation on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

stp mode

Syntax

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

undo stp mode

View

System view

Parameters

stp: Specifies the STP-compatible mode.

mstp: Specifies the MSTP mode.

rstp: Specifies the RSTP-compatible mode.

Description

Use the **stp mode** command to set the operating mode of an MSTP-enabled switch.

Use the **undo stp mode** command to restore the default operating mode of an MSTP-enabled switch.

By default, an MSTP-enabled switch operates in MSTP mode.

To make a switch compatible with STP and RSTP, MSTP provides following three operating modes.

- STP-compatible mode, where the ports of a switch send STP BPDUs to neighboring devices. If STP-enabled switches exist in a switched network, you can use the **stp mode stp** command to configure an MSTP-enabled switch to operate in STP-compatible mode.
- RSTP-compatible mode, where the ports of a switch send RSTP BPDUs to neighboring devices. If RSTP-enabled switches exist in a switched network, you can use the **stp mode rstp** command to configure an MSTP-enabled switch to operate in RSTP-compatible mode.
- MSTP mode, where the ports of a switch send MSTP BPDUs and STP BPDUs (if the switch is connected to STP-enabled switches) to neighboring devices. In this case, the switch is MSTP-capable.

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

Examples

Configure the MSTP operation mode as STP-compatible.

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

stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

View

Ethernet port view

Parameters

None

Description

Use the **stp no-agreement-check** command to enable the rapid transition feature on a port.

Use the **stp no-agreement-check** command to disable the rapid transition feature.

By default, the rapid transition feature is disabled on a port.

Some manufactures' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operates as the upstream switch of a 3com switch running MSTP, the upstream designated port fails to change their states rapidly.

The rapid transition feature aims to resolve this problem. When a 3com switch running MSTP is connected in the upstream direction to another manufacture's switch adopting proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the 3com switch operating as the downstream switch. Among these ports, those operating as the root ports will then actively send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Related commands: **stp interface no-agreement-check**.

Note

- The rapid transition feature can be enabled on only root ports or alternate ports.
- You can enable the rapid transition feature on the designated port. However, the feature does not take effect on the port.

Examples

Enable the rapid transition feature on GigabitEthernet 1/0/1.

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

Parameters

dot1d-1998: Uses the IEEE 802.1D-1998 standard to calculate the default path costs of ports.

dot1t: Uses the IEEE 802.1t standard to calculate the default path costs of ports.

legacy: Uses the proprietary standard to calculate the default path costs of ports.

Description

Use the **stp pathcost-standard** command to set the standard to be used to calculate the default path costs of the links connected to the switch.

Use the **undo stp pathcost-standard** command to specify to use the default standard.

By default, a switch uses the legacy standard to calculate the default path costs of ports.

Table 1-8 Link speeds and the corresponding path costs

Link speed	Operating mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
0	—	65,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	100 95 95 95	200,000 1,000,000 666,666 500,000	2,000 1,800 1,600 1,400
100 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	19 15 15 15	200,000 100,000 66,666 50,000	200 180 160 140
1,000 Mbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	4 3 3 3	200,000 10,000 6,666 5,000	20 18 16 14
10 Gbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	2 1 1 1	200,000 1,000 666 500	2 1 1 1

Normally, when a port operates in full-duplex mode, the corresponding path cost is slightly less than that when the port operates in half-duplex mode.

When the path cost of an aggregated link is calculated, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000 / link speed,

In this formula, the link speed is the sum of the speeds of the unblocked ports on the aggregated link, which is measured in 100 Kbps.

Examples

Configure to use the IEEE 802.1D-1998 standard to calculate the default path costs of ports.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp pathcost-standard dot1d-1998
```

Configure to use the IEEE 802.1t standard to calculate the default path costs of ports.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp pathcost-standard dot1t
```

stp point-to-point

Syntax

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

undo stp point-to-point

View

Ethernet port view

Parameters

force-true: Specifies that the link connected to the current Ethernet port is a point-to-point link.

force-false: Specifies that the link connected to the current Ethernet port is not a point-to-point link.

auto: Specifies to automatically determine whether or not the link connected to the current Ethernet port is a point-to-point link.

Description

Use the **stp point-to-point** command to specify whether the link connected to the current Ethernet port is a point-to-point link.

Use the **undo stp point-to-point** command to restore the link connected to the current Ethernet port to its default link type, which is automatically determined by MSTP.

By default, whether the link type of a port is point-to-point is automatically determined by the switch.

If no keyword is specified in the **stp point-to-point** command, the **auto** keyword is used by default, and so MSTP automatically determines the type of the link connected to the current port.

The rapid transition feature is not applicable to ports on non-point-to-point links.

If an Ethernet port is the master port of aggregation ports or operates in full-duplex mode, the link connected to the port is a point-to-point link. You are recommended to let MSTP automatically determine the link types of ports.

The two commands only apply to CISTs and MSTIs. If you configure the link to which a port is connected is a point-to-point link (or a non-point-to-point link), the configuration applies to all MSTIs (that is, the port is configured to connect to a point-to-point link (or a non-point-to-point link) in all MSTIs). If the actual physical link is not a point-to-point link and you configure the link to which the port is connected to be a point-to-point link, temporary loops may occur.

Related commands: **stp interface point-to-point**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp point-to-point force-true
```

stp port priority

Syntax

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

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

View

Ethernet port view

Parameters

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

port priority *priority*: Sets the port priority. The *priority* argument ranges from 0 to 240 and must be a multiple of 16 (such as 0, 16, and 32).

Description

Use the **stp port priority** command to set the port priority of the current port in the specified MSTI.

Use the **undo stp port priority** command to restore the default port priority of the current port in the specified MSTI.

The default port priority of a port in any MSTI is 128.

If you specify the *instance-id* argument to 0 or do not specify the argument, the two commands apply to the port priorities of ports on the CIST. The role a port plays in a MSTI is determined by the port priority in the instance. A port on a MSTP-enabled switch can have different port priorities and play different roles in different MSTIs. This enables packets of different VLANs to be forwarded along different physical links, so as to implement VLAN-based load balancing. Changing port priorities result in port role recalculation and state transition.

Related commands: **stp interface port priority**.

Examples

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

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 port priority 16
```

stp portlog

Syntax

stp [**instance** *instance-id*] **portlog**

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

View

System view

Parameters

instance *instance-id*: Specifies an MSTI ID, ranging from 0 to 16. The value of 0 indicates the CIST.

Description

Use the **stp portlog** command to enable log and trap message output for the ports of a specified instance.

Use the **undo stp portlog** command to disable this function.

By default, log and trap message output is disabled.

Executing the **stp portlog** command (without using the **instance** *instance-id* parameters) will enable log and trap message output for the ports of instance 0.

Examples

Enable log and trap message output for the ports of instance 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp instance 1 portlog
```

stp portlog all

Syntax

stp portlog all

undo stp portlog all

View

System view

Parameters

None

Description

Use the **stp portlog all** command to enable log and trap message output for the ports of all instances.

Use the **undo stp portlog all** command to disable this function.

By default, log and trap message output is disabled on the ports of all instances.

Examples

Enable log and trap message output for the ports of all instances.

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

stp priority

Syntax

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

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

View

System view

Parameters

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

priority: Switch priority to be set. This argument ranges from 0 to 61,440 and must be a multiple of 4,096 (such as 0, 4,096, and 8,192). There are totally 16 available switch priorities.

Description

Use the **stp priority** command to set the priority of the switch in the specified MSTI.

Use the **undo stp priority** command to restore the switch priority to the default priority in the specified MSTI.

The default priority of a switch is 32,768.

The priorities of switches are used for spanning tree calculation. Switch priorities are spanning tree-specific. That is, you can set different priorities for the same switch in different MSTIs.

If you do not specify the *instance-id* argument, the two commands apply to only the CIST.

Examples

Set the bridge priority of the switch in MSTI 1 to 4,096.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp instance 1 priority 4096
```

stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

View

System view

Parameters

None

Description

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

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

MST region-related parameters include: region name, revision level, and VLAN-to-MSTI mapping table. By default:

- MST region name is the first MAC address of the switch
- All VLANs are mapped to the CIST in the VLAN-to-MSTI mapping table
- The MSTP revision level is 0

You can modify the three parameters after entering MST region view by using the **stp region-configuration** command.

 **Note**

NTDP packets sent by devices in a cluster can be transmitted in only the instances where the management VLAN of the cluster resides.

Examples

Enter MST region view.

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

stp root primary

Syntax

stp [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum* [**hello-time** *centi-seconds*]]

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

View

System view

Parameters

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

bridgenum: Network diameter of the specified spanning tree. This argument ranges from 2 to 7 and defaults to 7.

centi-seconds: Hello time in centiseconds of the specified spanning tree. This argument ranges from 100 to 1,000 and defaults to 200.

Description

Use the **stp root primary** command to configure the current switch as the root bridge of a specified MSTI.

Use the **undo stp root** command to cancel the current configuration.

By default, a switch is not configured as a root bridge.

If you do not specify the *instance-id* argument, these two commands apply to only the CIST.

You can specify the current switch as the root bridge of an MSTI regardless of the priority of the switch. You can also specify the network diameter of the switched network by using the **stp root primary** command. The switch will then figure out the following three time parameters: hello time, forward delay, and max age. As the hello time figured out by the network diameter is not always the optimal one, you can set it manually through the **hello-time** *centi-seconds* parameter. Generally, you are recommended to obtain the forward delay and max age parameters through setting the network diameter.

 **Caution**

- You can configure only one root bridge for an MSTI and can configure one or more secondary root bridges for an MSTI. Specifying multiple root bridges for an MSTI causes unpredictable spanning tree calculation results.
- Once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Examples

Configure the current switch as the root bridge of MSTI 1, set the network diameter of the switched network to 4, and set the hello time to 500 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp instance 1 root primary bridge-diameter 4 hello-time 500
```

stp root secondary

Syntax

stp [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum* [**hello-time** *centi-seconds*]]

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

View

System view

Parameters

instance-id: MSTI ID ranging from 0 to 16. The value of 0 refers to the CIST.

bridgenum: Network diameter of the specified spanning tree. This argument ranges from 2 to 7 and defaults to 7.

centi-seconds: Hello time in centiseconds of the specified spanning tree. This argument ranges from 100 to 1,000 and defaults to 200.

Description

Use the **stp root secondary** command to configure the current switch as a secondary root bridge of a specified MSTI.

Use the **undo stp root** command to cancel the current configuration.

By default, a switch does not operate as a secondary root bridge.

If you do not specify the *instance-id* argument, the two commands apply to only the CIST.

You can configure one or more secondary root bridges for an MSTI. If the switch operating as the root bridge fails or is turned off, the secondary root bridge with the least MAC address becomes the root bridge.

You can specify the network diameter and the hello time of the switch when you are configuring it as a secondary root bridge. The switch will then figure out the other two time parameters: forward delay and max age. If the *instance-id* argument is specified to 0 in this command, the current switch is configured as the secondary root bridge of the CIST. You can configure only one root bridge for an MSTI but you can configure one or more secondary root bridges for an MSTI.

Once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Examples

Configure the current switch as a secondary root bridge of MSTI 4, setting the network diameter of the switched network to 5 and the hello time of the current switch to 300 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp instance 4 root secondary bridge-diameter 5 hello-time 300
```

stp root-protection

Syntax

stp root-protection

undo stp root-protection

View

Ethernet port view

Parameters

None

Description

Use the **stp root-protection** command to enable the root guard function on the current switch.

Use the **undo stp root-protection** command to restore the root guard function to the default state on the current switch.

By default, the root guard function is disabled.

Because of configuration errors or malicious attacks, the valid root bridge in the network may receive configuration BPDUs with their priorities higher than that of the root bridge, which causes new root bridge to be elected and network topology jitter to occur. In this case, flows that should have traveled along high-speed links are led to low-speed links, causing network congestion.

You can avoid this problem by utilizing the root guard function. Root-guard-enabled ports can only be kept as designated ports in all MSTIs. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state before it is specified as a non-designated port and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Related commands: **stp interface root-protection**.

Examples

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

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

Parameters

None

Description

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

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

By default, the TC-BPDU guard attack function is enabled, and the MAC address table and ARP entries can be removed for up to six times within 10 seconds.

Normally, a switch removes the MAC address table and ARP entries upon receiving TC-BPDUs. If a malicious user sends a large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing the MAC address table and ARP entries frequently, which may affect spanning tree calculation, occupy large amount of bandwidth and increase switch CPU utilization.

With the TC-BPDU attack guard function enabled, a switch performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the switch only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a switch from being busy in removing the MAC address table and ARP entries.

Examples

Enable the TC-BPDU attack guard function on the switch.

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

stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

View

System view

Parameters

number: Maximum number of times that a switch can remove the MAC address table and ARP entries within each 10 seconds, in the range of 1 to 255.

Description

Use the **stp tc-protection threshold** command to set the maximum number of times that a switch can remove the MAC address table and ARP entries within each 10 seconds.

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

Normally, a switch removes the MAC address table and ARP entries upon receiving a TC-BPDU. If a malicious user sends large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing the MAC address table and ARP entries, which may affect spanning tree calculation, occupy a large amount of bandwidth and increase switch CPU utilization.

With the TC-BPDU attack guard function enabled, a switch performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the switch only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a switch from being busy in removing the MAC address table and ARP entries.

You can use the **stp tc-protection threshold** command to set the maximum times for a switch to remove the MAC address table and ARP entries in a specific period. When the number of the TC-BPDUs received within a period is less than the maximum times, the switch performs a removing operation upon receiving a TC-BPDU. After the number of the TC-BPDUs received reaches the maximum times, the switch stops performing the removing operation. For example, if you set the maximum times for a switch to remove the MAC address table and ARP entries to 100 and the switch receives 200 TC-BPDUs in the period, the switch removes the MAC address table and ARP entries for only 100 times within the period.

Examples

Set the maximum times for a switch to remove the MAC address table and ARP entries within 10 seconds to 5.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp tc-protection threshold 5
```

stp timer forward-delay

Syntax

stp timer forward-delay *centi-seconds*

undo stp timer forward-delay

View

System view

Parameters

centi-seconds: Forward delay in centiseconds to be set. This argument ranges from 400 to 3,000.

Description

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

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

By default, the forward delay of the switch is 1,500 centiseconds.

To prevent the occurrence of temporary loops, when a port changes its state from discarding to forwarding, it undergoes an intermediate state and waits for a specific period to synchronize with the state transition of the remote switches. This state transition period is determined by the forward delay configured on the root bridge.

The forward delay setting configured on a root bridge applies to all non-root bridges.

As for the configuration of the three time-related parameters (namely, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay – 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically calculated by MSTP.

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

Examples

Set the forward delay to 2,000 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp timer forward-delay 2000
```

stp timer hello

Syntax

stp timer hello *centi-seconds*

undo stp timer hello

View

System view

Parameters

centi-seconds: Hello time to be set, in the range of 100 to 1,000 (in centiseconds).

Description

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

Use the **undo stp timer hello** command to restore the hello time of the switch to the default value.

By default, the hello time of the switch is 200 centiseconds.

A root bridge regularly sends out configuration BPDUs to maintain the stability of existing spanning trees. If the switch does not receive BPDU packets in a specified period, spanning trees will be recalculated because BPDU packets time out. When a switch becomes a root bridge, it regularly sends BPDUs at the interval specified by the hello time you have configured on it. The other none-root-bridge switches adopt the interval specified by the hello time.

As for the configuration of the three time-related parameters (namely, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 × (forward delay – 1 second) >= max age

Max age >= 2 × (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically calculated by MSTP.

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

Examples

Set the hello time to 400 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp timer hello 400
```

stp timer max-age

Syntax

stp timer max-age *centi-seconds*

undo stp timer max-age

View

System view

Parameters

centi-seconds: Max age to be set, in the range of 600 to 4,000 (in centiseconds).

Description

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

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

By default, the max age of a switch is 2,000 centiseconds.

MSTP is capable of detecting link failures and automatically restoring redundant links to the forwarding state. In CIST, switches use the max age parameter to judge whether or not a received configuration BPDU times out. Spanning trees will be recalculated if a configuration BPDU received by a port times out.

The max age is meaningless to MSTIs. The max age configured for the root bridge of the CIST applies to all switches operating on the CIST, including the root bridge.

As for the configuration of the three time-related parameters (namely, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter:

2 × (forward delay – 1 second) >= max age,

Max age >= 2 × (hello time + 1 second).

You are recommended to specify the network diameter of the switched network and the hello time parameter by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically determined by MSTP.

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

Examples

Set the max age to 1,000 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp timer max-age 1000
```

stp timer-factor

Syntax

stp timer-factor *number*

undo stp timer-factor

View

System view

Parameters

number: Hello time factor to be set, in the range of 1 to 10.

Description

Use the **stp timer-factor** command to set the timeout time of a switch in the form of a multiple of the hello time.

Use the **undo stp timer-factor** command to restore the hello time factor to the default value.

By default, the hello time factor of the switch is 3.

A switch regularly sends protocol packets to its neighboring devices at the interval specified by the hello time parameter to test the links. Generally, a switch regards its upstream switch faulty if the former does receive any protocol packets from the latter in a period three times of the hello time and then initiates the spanning tree recalculation process.

Spanning trees may be recalculated even in a steady network if an upstream switch is always busy. You can configure the hello time factor to a larger number to avoid this problem. Normally, the timeout time can be four (or more) times of the hello time. For a steady network, the timeout time can be five to seven times of the hello time.

Examples

Set the hello time factor to 7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax

stp transmit-limit *packetnum*

undo stp transmit-limit

View

Ethernet port view

Parameters

packetnum: Maximum number of configuration BPDUs a port can transmit in each hello time. This argument ranges from 1 to 255.

Description

Use the **stp transmit-limit** command to set the maximum number of configuration BPDUs the current port can transmit in each hello time.

Use the **undo stp transmit-limit** command to restore the maximum number to the default value.

By default, the maximum number of configuration BPDUs a port can transmit in each hello time is 10.

A larger number configured by the **stp transmit-limit** command allows more configuration BPDUs to be transmitted in each hello time, which may occupy more switch resources. So you are recommended configure it to a proper value to avoid network topology jitter and prevent MSTP from occupying too many bandwidth resources.

Related commands: **stp interface transmit-limit**.

Examples

Set the maximum number of configuration BPDUs that can be transmitted through GigabitEthernet 1/0/1 in each hello time to 15.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 15
```

vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

View

MST region view

Parameters

modulo: Modulo by which VLANs are mapped to MSTIs, in the range of 1 to 16.

Description

Use the **vlan-mapping modulo** command to set the modulo by which VLANs are mapped to MSTIs.

By default, all VLANs in a network are mapped to the CIST (MSTI 0).

MSTP uses a VLAN-to-MSTI mapping table to describe VLAN-to-MSTI mappings. You can use this command to establish the VLAN-to-MSTI mapping table and map VLANs to MSTIs in a specific way.

Note that a VLAN cannot be mapped to multiple different MSTIs at the same time. A VLAN-to-MSTI mapping becomes invalid when you map the VLAN to another MSTI.

Note

You can map VLANs to the specific MSTIs rapidly by using the **vlan-mapping modulo** *modulo* command. The ID of the MSTI to which a VLAN is mapped can be figured out by using the following formula:

(VLAN ID-1) % *modulo* + 1.

In this formula, (VLAN ID-1) % *modulo* yields the module of (VLAN ID-1) with regards to the *modulo* argument. For example, if you set the *modulo* argument to 16, then VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to MSTI 2, …, VLAN 16 is mapped to MSTI 16, VLAN 17 is mapped to MSTI 1, and so on.

Related commands: **check region-configuration**, **revision-level**, **region-name**, **active region-configuration**.

Examples

Map VLANs to MSTIs, with the modulo being 16.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 16
```

vlan-vpn tunnel

Syntax

vlan-vpn tunnel

undo vlan-vpn tunnel

View

System view

Parameters

None

Description

Use the **vlan-vpn tunnel** command to enable the VLAN-VPN tunnel function for a switch.

Use the **undo vlan-vpn tunnel** command to disable the VLAN-VPN tunnel function.

The VLAN-VPN tunnel function enables BPDUs to be transparently transmitted between geographically dispersed user networks through specified VLAN VPNs in operator's networks, through which spanning trees can be calculated across these user networks and are independent of those of the operator's network.

By default, the VLAN-VPN tunnel function is disabled.

Note

- The VLAN-VPN tunnel function can only be enabled on STP-enabled devices.
- To enable the VLAN-VPN tunnel function, make sure the links between operator's networks are trunk links.
- If a fabric port exists on a switch, you cannot enable the VLAN-VPN function for any port of the switch.

Examples

Enable the VLAN-VPN tunnel function for the switch.

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

Table of Contents

1 802.1x Configuration Commands

802.1x Configuration Commands

display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-list*]

View

Any view

Parameters

sessions: Displays the information about 802.1x sessions.

statistics: Displays the statistics on 802.1x.

interface: Display the 802.1x-related information about a specified port.

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **display dot1x** command to display 802.1x-related information, such as configuration information, operation information (session information), and statistics.

When the *interface-list* argument is not provided, this command displays 802.1x-related information about all the ports.

The output information can be used to verify 802.1 x-related configurations and to troubleshoot.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, **dot1x timer**.

Examples

Display 802.1x-related information.

```
<Sysname> display dot1x
Global 802.1X protocol is enabled
 CHAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled
```

```
 Configuration: Transmit Period     30 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
  EAD Quick Deploy configuration:
                Url: http: //192.168.19.23
                Free-ip: 192.168.19.0 255.255.255.0
                Acl-timeout:   30 m

 Total maximum 802.1x user resource number is 1024
 Total current used 802.1x resource number is 1

 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Proxy trap checker is disabled
   Proxy logoff checker is disabled
   Version-Check is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Port-based
   ReAuthenticate is disabled
   Max number of on-line users is 256

   Authentication Success: 4, Failed: 2
   EAPOL Packets: Tx 7991, Rx 14
   Sent EAP Request/Identity Packets : 7981
        EAP Request/Challenge Packets: 0
   Received EAPOL Start Packets : 5
            EAPOL LogOff Packets: 1
            EAP Response/Identity Packets : 4
            EAP Response/Challenge Packets: 4
            Error Packets: 0
 1. Authenticated user : MAC address: 000d-88f6-44c1

   Controlled User(s) amount to 1

GigabitEthernet1/0/2
……
```

Table 1-1 Description on the fields of the **display dot1x** command

Field	Description
Equipment 802.1X protocol is enabled	802.1x protocol (802.1x for short) is enabled on the switch.
CHAP authentication is enabled	CHAP authentication is enabled.

Field	Description
DHCP-launch is disabled	DHCP-triggered. 802.1x authentication is disabled.
Handshake is enabled	The online user handshaking function is enabled.
Proxy trap checker is disabled	Whether or not to send Trap packets when detecting a supplicant system logs in through a proxy. • Disable means the switch does not send Trap packets when it detects that a supplicant system logs in through a proxy. • Enable means the switch sends Trap packets when it detects that a supplicant system logs in through a proxy.
Proxy logoff checker is disabled	Whether or not to disconnect a supplicant system when detecting it logs in through a proxy. • Disable means the switch does not disconnect a supplicant system when it detects that the latter logs in through a proxy. • Enable means the switch disconnects a supplicant system when it detects that the latter logs in through a proxy.
EAD Quick Deploy is enabled	Quick EAD deployment is enabled.
Transmit Period	Setting of the Transmission period timer (the tx-period)
Handshake Period	Setting of the handshake period timer (the handshake-period)
ReAuth Period	Re-authentication interval
ReAuth MaxTimes	Maximum times of re-authentications
Quiet Period	Setting of the quiet period timer (the quiet-period)
Quiet Period Timer is disabled	The quiet period timer is disabled here. It can also be configured as enabled when necessary.
Supp Timeout	Setting of the supplicant timeout timer (supp-timeout)
Server Timeout	Setting of the server-timeout timer (server-timeout)
The maximal retransmitting times	The maximum number of times that a switch can send authentication request packets to a supplicant system
Url	URL for HTTP redirection
Free-ip	Free IP range that users can access before passing authentication
Acl-timeout	ACL timeout period
Total maximum 802.1x user resource number	The maximum number of 802.1x users that a switch can accommodate
Total current used 802.1x resource number	The number of online supplicant systems
GigabitEthernet1/0/1 is link-down	GigabitEthernet 1/0/1 port is down.

Field	Description
802.1X protocol is disabled	802.1x is disabled on the port
Proxy trap checker is disabled	Whether or not to send Trap packets when detecting a supplicant system in logging in through a proxy. • Disable means the switch does not send Trap packets when it detects that a supplicant system logs in through a proxy. • Enable means the switch sends Trap packets when it detects that a supplicant system logs in through a proxy.
Proxy logoff checker is disabled	Whether or not to disconnect a supplicant system when detecting it in logging in through a proxy. • Disable means the switch does not disconnect a supplicant system when it detects that the latter logs in through a proxy. • Enable means the switch disconnects a supplicant system when it detects that the latter logs in through a proxy.
Version-Check is disabled	Whether or not the client version checking function is enabled: • Disable means the switch does not checks client version. • Enable means the switch checks client version.
The port is an authenticator	The port acts as an authenticator system.
Authentication Mode is Auto	The port access control mode is **Auto**.
Port Control Type is Mac-based	The access control method of the port is MAC-based. That is, supplicant systems are authenticated based on their MAC addresses.
ReAuthenticate is disabled	802.1x re-authentication is disabled on the port.
Max number of on-line users	The maximum number of online users that the port can accommodate
…	Information omitted here

dot1x

Syntax

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet

port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x** command to enable 802.1x globally or for specified Ethernet ports.

Use the **undo dot1x** command to disable 802.1x globally or for specified Ethernet ports.

By default, 802.1x is disabled globally and also on all ports.

In system view:

- If you do not provide the *interface-list* argument, the **dot1x** command enables 802.1x globally.
- If you specify the *interface-list* argument, the **dot1x** command enables 802.1x for the specified Ethernet ports.

In Ethernet port view, the *interface-list* argument is not available and the command enables 802.1x for only the current Ethernet port.

802.1x-related configurations take effect on a port only after 802.1x is enabled both globally and on the port.

Note

- The settings of 802.1x and MAC address learning limit are mutually exclusive. Enabling 802.1x on a port will prevent you from setting the limit on MAC address learning on the port and vice versa.
- The settings of 802.1x and aggregation group member are mutually exclusive. Enabling 802.1x on a port will prevent you from adding the port to an aggregation group and vice versa.

Related commands: **display dot1x**.

Examples

Enable 802.1x for GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x interface GigabitEthernet 1/0/1
```

Enable 802.1x globally.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x
```

dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

View

System view

Parameters

chap: Authenticates using challenge handshake authentication protocol (CHAP).

pap: Authenticates using password authentication protocol (PAP).

eap: Authenticates using extensible authentication protocol (EAP).

Description

Use the **dot1x authentication-method** command to set the 802.1x authentication method.

Use the **undo dot1x authentication-method** command to revert to the default 802.1x authentication method.

The default 802.1x authentication method is CHAP.

PAP applies a two-way handshaking procedure. In this method, passwords are transmitted in plain text.

CHAP applies a three-way handshaking procedure. In this method, user names are transmitted rather than passwords. Therefore this method is safer.

In EAP authentication, a switch authenticates supplicant systems by encapsulating 802.1x authentication information in EAP packets and sending the packets to the RADIUS server, instead of converting the packets into RADIUS packets before forwarding to the RADIUS server. You can use EAP authentication in one of the four sub-methods: PEAP, EAP-TLS, EAP-TTLS and EAP-MD5.

Related commands: **display dot1x**.

Note

When the current device operates as the authentication server, EAP authentication is unavailable.

Examples

Specify the authentication method to **PAP**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x authentication-method pap
```

dot1x dhcp-launch

Syntax

dot1x dhcp-launch

undo dot1x dhcp-launch

View

System view

Parameters

None

Description

Use the **dot1x dhcp-launch** command to specify an 802.1x-enabled switch to launch the process to authenticate a supplicant system when the supplicant system applies for a dynamic IP address through DHCP.

Use the **undo dot1x dhcp-launch** command to disable an 802.1x-enabled switch from authenticating a supplicant system when the supplicant system applies for a dynamic IP address through DHCP.

By default, an 802.1x-enabled switch does not authenticate a supplicant system when the latter applies for a dynamic IP address through DHCP.

Related commands: **display dot1x**.

Examples

Configure to authenticate a supplicant system when it applies for a dynamic IP address through DHCP.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x dhcp-launch
```

dot1x guest-vlan

Syntax

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

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

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x guest-vlan** command to enable the guest VLAN function for ports.

Use the **undo dot1x guest-vlan** command to disable the guest VLAN function for ports.

After 802.1x and guest VLAN are properly configured on a port:

- If the switch receives no response from the port after sending EAP-Request/Identity packets to the port for the maximum number of times, the switch will add the port to the guest VLAN.
- Users in a guest VLAN can access the guest VLAN resources without 802.1x authentication. However, they have to pass the 802.1x authentication to access the external resources.

In system view,

- If you do not provide the *interface-list* argument, these two commands apply to all the ports of the switch.
- If you specify the *interface-list* argument, these two commands apply to the specified ports.

In Ethernet port view, the *interface-list* argument is not available and these two commands apply to only the current Ethernet port.

Caution

- The guest VLAN function is available only when the switch operates in the port-based authentication mode.
- Only one guest VLAN can be configured on a switch.
- The guest VLAN function is unavailable when the **dot1x dhcp-launch** command is executed on the switch, because the switch does not send authentication request packets in this case.

Examples

Configure the switch to operate in the port-based authentication mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x port-method portbased
```

Enable the guest VLAN function for all the ports.

```
[Sysname] dot1x guest-vlan 1
```

dot1x handshake

Syntax

dot1x handshake enable

undo dot1x handshake enable

View

System view

Parameters

None

Description

Use the **dot1x handshake enable** command to enable the online user handshaking function.

Use the **undo dot1x handshake enable** command to disable the online user handshaking function.

By default, the online user handshaking function is enabled.

Caution

- To enable the proxy detecting function, you need to enable the online user handshaking function first.
- With the support of H3C proprietary clients, handshaking packets can be used to test whether or not a user is online.
- As clients that are not of H3C do not support the online user handshaking function, switches cannot receive handshaking acknowledgement packets from them in handshaking periods. To prevent users being falsely considered offline, you need to disable the online user handshaking function in this case.

Examples

Enable the online user handshaking function.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x handshake enable
```

dot1x handshake secure

Syntax

dot1x handshake secure

undo dot1x handshake secure

View

Ethernet port view

Parameters

None

Description

Use the **dot1x handshake secure** command to enable the handshaking packet protection function, protecting the device against attacks from fake clients.

Use the **undo dot1x handshake secure** command to disable the handshaking packet protection function.

By default, the handshaking packet protection function is disabled.

Caution

The handshaking packet protection function requires the cooperation of the client and the authentication server. If either of the two ends does not support the function, you need to disable it on the other one.

Examples

Enable the handshaking packet protection function.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake secure
```

dot1x max-user

Syntax

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

user-number: Maximum number of users a port can accommodate, in the range 1 to 256.

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x max-user** command to set the maximum number of users an Ethernet port can accommodate.

Use the **undo dot1x max-user** command to revert to the default maximum user number.

By default, a port can accommodate up to 256 users.

In system view:

- If you do not provide the *interface-list* argument, these two commands apply to all the ports of the switch.
- If you specify the *interface-list* argument, these two commands apply to the specified ports.

In Ethernet port view, the *interface-list* argument is not available and the commands apply to only the current port.

Related commands: **display dot1x**.

Examples

Configure the maximum number of users that GigabitEthernet 1/01 port can accommodate to be 32.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x max-user 32 interface GigabitEthernet 1/0/1
```

dot1x port-control

Syntax

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

auto: Specifies to operate in **auto** access control mode. When a port operates in this mode, all the unauthenticated hosts connected to it are unauthorized. In this case, only EAPoL packets can be exchanged between the switch and the hosts. And the hosts connected to the port are authorized to access the network resources after the hosts pass the authentication. Normally, a port operates in this mode.

authorized-force: Specifies to operate in **authorized-force** access control mode. When a port operates in this mode, all the hosts connected to it can access the network resources without being authenticated.

unauthorized-force: Specifies to operate in **unauthorized-force** access control mode. When a port operates in this mode, the hosts connected to it cannot access the network resources.

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x port-control** command to specify the access control mode for specified Ethernet ports.

Use the **undo dot1x port-control** command to revert to the default access control mode.

The default access control mode is **auto**.

Use the **dot1x port-control** command to configure the access control mode for specified 802.1x-enabled ports.

In system view:

- If you do not provide the *interface-list* argument, these two commands apply to all the ports of the switch.
- If you specify the *interface-list* argument, these commands apply to the specified ports.

In Ethernet port view, the *interface-list* argument is not available and the commands apply to only the current Ethernet port.

Related commands: **display dot1x**.

Examples

Specify GigabitEthernet 1/0/1 to operate in **unauthorized-force** access control mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x port-control unauthorized-force interface GigabitEthernet 1/0/1
```

dot1x port-method

Syntax

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

macbased: Performs MAC-based authentication.

portbased: Performs port-based authentication.

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string "&<1-10>" means that up to 10 port lists can be provided.

Description

Use the **dot1x port-method** command to specify the access control method for specified Ethernet ports.

Use the **undo dot1x port-method** command to revert to the default access control method.

By default, the access control method is **macbased**.

This command specifies the way in which the users are authenticated.

- In MAC-based authentication mode, the users connected to the port are authenticated separately. Thus, log-off of a user will not affect other users.
- In port-based authentication mode, all the users connected to the port can access the network without being authenticated if a user among them passes the authentication. When the user logs off, the network is inaccessible to all other supplicant systems too.
- Changing the access control method on a port by the dot1x port-method command will forcibly log out the online 802.1x users on the port.

In system view:

- If you do not provide the *interface-list* argument, these two commands apply to all the ports of the switch.
- If you specify the *interface-list* argument, these commands apply to the specified ports.

In Ethernet port view, the *interface-list* argument is not available and the commands apply to only the current Ethernet port.

Related commands: **display dot1x**.

Examples

Specify to authenticate users connected to GigabitEthernet 1/0/1 by port numbers.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x port-method portbased interface GigabitEthernet 1/0/1
```

dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

View

System view

Parameters

None

Description

Use the **dot1x quiet-period** command to enable the quiet-period timer.

Use the **undo dot1x quiet-period** command to disable the quiet-period timer.

When a user fails to pass the authentication, the authenticator system (such as a 3Com switch) will stay quiet for a period (determined by the quiet-period timer) before it performs another authentication. During the quiet period, the authenticator system performs no 802.1x authentication of the user.

By default, the quiet-period timer is disabled.

Related commands: **display dot1x**, **dot1x timer**.

Examples

Enable the quiet-period timer.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x quiet-period
```

dot1x retry

Syntax

dot1x retry *max-retry-value*

undo dot1x retry

View

System view

Parameters

max-retry-value: Maximum number of times that a switch sends authentication request packets to a user. This argument ranges from 1 to 10.

Description

Use the **dot1x retry** command to specify the maximum number of times that a switch sends authentication request packets to a user.

Use the **undo dot1x retry** command to revert to the default value.

By default, a switch sends authentication request packets to a user for up to 2 times.

After a switch sends an authentication request packet to a user, it sends another authentication request packet if it does not receive response from the user after a specific period of time. If the switch still receives no response when the configured maximum number of authentication request transmission attempts is reached, it stops sending requests to the user. This command applies to all ports.

Related commands: **display dot1x**.

Examples

Specify the maximum number of times that the switch sends authentication request packets to be 9.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x retry 9
```

dot1x retry-version-max

Syntax

dot1x retry-version-max *max-retry-version-value*

undo dot1x retry-version-max

View

System view

Parameters

max-retry-version-value: Maximum number of times that a switch sends version request packets to a user. This argument ranges from 1 to 10.

Description

Use the **dot1x retry-version-max** command to set the maximum number of times that a switch sends version request packets to a user.

Use the **undo dot1x retry-version-max** command to revert to the default value.

By default, a switch sends version request packets to a user for up to 3 times.

After a switch sends a version request packet to a user, it sends another version request packet if it does receive response from the user after a specific period of time (as determined by the client version request timer). When the number set by this command has reached and there is still no response from the user, the switch continues the following authentication procedures without sending version requests. This command applies to all the ports with the version checking function enabled.

Related commands: **display dot1x**, **dot1x timer**.

Examples

Configure the maximum number of times that the switch sends version request packets to 6.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x retry-version-max 6
```

dot1x re-authenticate

Syntax

dot1x re-authenticate [**interface** *interface-list*]

undo dot1x re-authenticate [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string "&<1-10>" means that up to 10 port lists can be provided.

Description

Use the **dot1x re-authenticate** command to enable 802.1x re-authentication on specific ports or on all ports of the switch.

Use the **undo dot1x re-authenticate** command to disable 802.1x re-authentication on specific ports or on all ports of the switch.

By default, 802.1x re-authentication is disabled on all ports.

In system view:

- If you do not specify the *interface-list* argument, this command will enable 802.1x re-authentication on all ports.
- If you specify the *interface-list* argument, the command will enable 802.1x on the specified ports.

In Ethernet port view, the *interface-list* argument is not available and 8021.x re-authentication is enabled on the current port only.

Note

802.1x must be enabled globally and on the current port before 802.1x re-authentication can be configured on a port.

Examples

Enable 802.1x re-authentication on port GigabitEthernet 1/0/1.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] dot1x
 802.1X is enabled globally.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
 802.1X is enabled on port GigabitEthernet1/0/1 already.
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
 Re-authentication is enabled on port GigabitEthernet1/0/1
```

dot1x supp-proxy-check

Syntax

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

logoff: Disconnects a user upon detecting it logging in through a proxy or through multiple network adapters.

trap: Sends Trap packets upon detecting a user logging in through a proxy or through multiple network adapters.

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x supp-proxy-check** command to enable 802.1x proxy checking for specified ports.

Use the **undo dot1x supp-proxy-check** command to disable 802.1x proxy checking for specified ports.

By default, 802.1x proxy checking is disabled on all Ethernet ports.

In system view:

- If you do not specify the *interface-list* argument, the configurations performed by these two commands are global.
- If you specify the *interface-list* argument, these two commands apply to the specified Ethernet ports.

In Ethernet port view, the *interface-list* argument is not available and the commands apply to only the current Ethernet port.

The proxy checking function takes effect on a port only when the function is enabled both globally and on the port.

802.1x proxy checking checks for:

- Users logging in through proxies
- Users logging in through IE proxies

- Whether or not a user logs in through multiple network adapters (that is, when the user attempts to log in, it contains more than one active network adapters.)

A switch can optionally take the following actions in response to any of the above three cases:

- Only disconnects the user but sends no Trap packets, which can be achieved by using the **dot1x supp-proxy-check logoff** command.
- Sends Trap packets without disconnecting the user, which can be achieved by using the **dot1x supp-proxy-check trap** command.

This function needs the cooperation of 802.1x clients and the CAMS server:

- Multiple network adapter checking, proxy checking, and IE proxy checking are enabled on the 802.1x client.
- The CAMS server is configured to disable the use of multiple network adapters, proxies, and IE proxy.

By default, proxy checking is disabled on 802.1x client. In this case, if you configure the CAMS server to disable the use of multiple network adapters, proxies, and IE proxy, it sends messages to the 802.1x client to ask the latter to disable the use of multiple network adapters, proxies, and IE proxy after the user passes the authentication.

Note

- The 802.1x proxy checking function needs the cooperation of H3C's 802.1x client program.
- The proxy checking function takes effect only after the client version checking function is enabled on the switch (using the **dot1x version-check** command).

Related commands: **display dot1x**.

Examples

Configure to disconnect the users connected to GigabitEthernet 1/0/1 through GigabitEthernet 1/0/8 ports if they are detected logging in through proxies.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface GigabitEthernet 1/0/1 to GigabitEthernet 1/0/8
```

Configure the switch to send Trap packets if the users connected to GigabitEthernet 1/0/9 port is detected logging in through proxies.

```
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface GigabitEthernet 1/0/9
```

dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **ver-period** *ver-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **server-timeout** | **supp-timeout** | **tx-period** | **ver-period** }

View

System view

Parameters

handshake-period *handshake-period-value*: Sets the handshake timer. This timer sets the handshake-period and is triggered after a supplicant system passes the authentication. It sets the interval for a switch to send handshake request packets to online users. If you set the number of retries to N by using the **dot1x retry** command, an online user is considered offline when the switch does not receive response packets from it in a period N times of the handshake-period.

The *handshake-period-value* argument ranges from 5 to 1,024 (in seconds). By default, the handshake timer is set to 15 seconds.

quiet-period *quiet-period-value*: Sets the quiet-period timer. This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system.

The *quiet-period-value* argument ranges from 10 to 120 (in seconds). By default, the quiet-period timer is set to 60 seconds.

server-timeout *server-timeout-value*: Sets the RADIUS server timer. This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, a switch sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.

The *server-timeout-value* argument ranges from 100 to 300 (in seconds). By default, the RADIUS server timer is set to 100 seconds.

supp-timeout *supp-timeout-value*: Sets the supplicant system timer. This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system (The packet is used to request the supplicant system for the MD5 encrypted string.) The switch sends another request/challenge packet to the supplicant system if the switch does not receive the response from the supplicant system when this timer times out..

The *supp-timeout-value* argument ranges from 10 to 120 (in seconds). By default, the supplicant system timer is set to 30 seconds.

tx-period *tx-period-value*: Sets the transmission timer. This timer sets the tx-period and is triggered in two cases. The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch

authenticates the 802.1x client who cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets.

The *tx-period-value* argument ranges from 1 to 120 (in seconds). By default, the transmission timer is set to 30 seconds.

ver-period *ver-period-value*: Sets the client version request timer. This timer sets the version period and is triggered after a switch sends a version request packet. The switch sends another version request packet if it does receive version response packets from the supplicant system when the timer expires.

The *ver-period-value* argument ranges from 1 to 30 (in seconds). By default, the client version request timer is set to 30 seconds.

Description

Use the **dot1x timer** command to set a specified 802.1x timer.

Use the **undo dot1x timer** command to restore a specified 802.1x timer to the default setting.

During an 802.1x authentication process, multiple timers are triggered to ensure that the supplicant systems, the authenticator systems, and the Authentication servers interact with each other in an orderly way. To make authentications being processed in the desired way, you can use the **dot1x timer** command to set the timers as needed. This may be necessary in some special situations or in tough network environments. Normally, the defaults are recommended. (Note that some timers cannot be adjusted.)

Related commands: **display dot1x**.

Examples

Set the RADIUS server timer to 150 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x timer server-timeout 150
```

dot1x timer reauth-period

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

View

System view

Parameters

reauth-period *reauth-period-value*: Specifies re-authentication interval, in seconds. After this timer expires, the switch initiates 802.1x re-authentication. The value of the *reauth-period-value* argument ranges from 60 to 7,200.

Description

Use the **dot1x timer reauth-period** command to configure the interval for 802.1x re-authentication.

Use the **undo dot1x timer reauth-period** command to restore the default 802.1x re-authentication interval.

By default, the 802.1x re-authentication interval is 3,600 seconds.

Examples

Set the 802.1x re-authentication interval to 150 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x timer reauth-period 150
```

dot1x version-check

Syntax

dot1x version-check [**interface** *interface-list*]

undo dot1x version-check [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **dot1x version-check** command to enable 802.1x client version checking for specified Ethernet ports.

Use the **undo dot1x version-check** command to disable 802.1x client version checking for specified Ethernet ports.

By default, 802.1x client version checking is disabled on all the Ethernet ports.

In system view:

- If you do not provide the *interface-list* argument, these two commands apply to all the ports of the switch.
- If you specify the *interface-list* argument, these commands apply to the specified ports.

In Ethernet port view, the *interface-list* argument is not available and the commands apply to only the current Ethernet port.

Examples

Configure GigabitEthernet 1/0/1 to check the version of the 802.1x client upon receiving authentication packets.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x version-check
```

reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-list*]

View

User view

Parameters

interface-list: Ethernet port list, in the form of *interface-list*= { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, in which *interface-type* specifies the type of an Ethernet port and *interface-number* is the number of the port. The string “&<1-10>” means that up to 10 port lists can be provided.

Description

Use the **reset dot1x statistics** command to clear 802.1x-related statistics.

To retrieve the latest 802.1x-related statistics, you can use this command to clear the existing 802.1x-related statistics first.

When you execute this command,

If the *interface-list* argument is not specified, this command clears the global 802.1x statistics and the 802.1x statistics on all the ports.

If the *interface-list* argument is specified, this command clears the 802.1x statistics on the specified ports.

Related commands: **display dot1x**.

Examples

Clear 802.1x statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface GigabitEthernet 1/0/1
```

2 Quick EAD Deployment Configuration Commands

Quick EAD Deployment Configuration Commands

dot1x free-ip

Syntax

dot1x free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x free-ip [*ip-address* { *mask-address* | *mask-length* }]

View

System view

Parameters

ip-address: Free IP address, in dotted decimal notation.

mask-address: Subnet mask of the free IP address, in dotted decimal notation.

mask-length: Length of the subnet mask of the free IP address, in the range 0 to 32.

Description

Use the **dot1x free-ip** command to configure a free IP range. A free IP range is an IP range that users can access before passing 802.1x authentication.

Use the **undo dot1x free-ip** command to remove a specified free IP range or all free IP ranges.

By default, no free IP range is configured.

Note

- You must configure the URL for HTTP redirection before configuring a free IP range.
- The device supports up to two free IP ranges.

Examples

Configure a free IP range for users to access before passing authentication.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x free-ip 192.168.19.23 24
```

dot1x timer acl-timeout

Syntax

dot1x timer acl-timeout *acl-timeout-value*

undo dot1x timer acl-timeout

View

System view

Parameters

acl-timeout-value: ACL timeout period (in minutes), in the range of 1 to 1440.

Description

Use the **dot1x timer acl-timeout** command to configure the ACL timeout period.

Use the **undo dot1x timer acl-timeout** command to restore the default.

By default, the ACL timeout period is 30 minutes.

Related commands: dot1x configuration commands.

Examples

Set the ACL timeout period to 40 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x timer acl-timeout 40
```

dot1x url

Syntax

dot1x url *url-string*

undo dot1x url

View

System view

Parameters

url-string: URL for HTTP redirection, in the format of http://*x.x.x.x*.

Description

Use the **dot1x url** command to configure the URL for HTTP redirection.

Use the **undo dot1x url** command to remove the configuration.

By default, no URL is configured for HTTP redirection.

Related commands: dot1x configuration commands.

Examples

Configure the URL for HTTP redirection.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] dot1x url http://192.168.19.23
```

3 HABP Configuration Commands

HABP Configuration Commands

display habp

Syntax

display habp

View

Any view

Parameters

None

Description

Use the **display habp** command to display HABP configuration and status.

Examples

Display HABP configuration and status.

```
<Sysname> display habp
Global HABP information:
        HABP Mode: Server
        Sending HABP request packets every 20 seconds
        Bypass VLAN: 2
```

Table 3-1 Description on the fields of the **display habp** command

Field	Description
HABP Mode	Indicates the HABP mode of the switch. A switch can operate as an HABP server (displayed as Server) or an HABP client (displayed as Client).
Sending HABP request packets every 20 seconds	The HABP request packet transmission interval is 20 seconds.
Bypass VLAN	Indicates the IDs of the VLANs to which HABP request packets are sent.

display habp table

Syntax

display habp table

View

Any view

Parameters

None

Description

Use the **display habp table** command to display the MAC address table maintained by HABP.

Examples

Display the MAC address table maintained by HABP.

```
<Sysname> display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        GigabitEthernet1/0/1
```

Table 3-2 Description on the fields of the **display habp table** command

Field	Description
MAC	MAC addresses contained in the HABP MAC address table.
Holdtime	Hold time of the entries in the HABP MAC address table. An entry is removed from the table if it is not updated in a period determined by the hold time.
Receive Port	The port from which a MAC address is learned

display habp traffic

Syntax

display habp traffic

View

Any view

Parameters

None

Description

Use the **display habp traffic** command to display the statistics on HABP packets.

Examples

Display the statistics on HABP packets.

```
<Sysname> display habp traffic
```

```
HABP counters :
        Packets output: 0, Input: 0
        ID error: 0, Type error: 0, Version error: 0
        Sent failed: 0
```

Table 3-3 Description on the fields of the **display habp traffic** command

Field	Description
Packets output	Number of the HABP packets sent
Input	Number of the HABP packets received
ID error	Number of the HABP packets with ID errors
Type error	Number of the HABP packets with type errors
Version error	Number of the HABP packets with version errors
Sent failed	Number of the HABP packets that failed to be sent

habp enable

Syntax

habp enable

undo habp enable

View

System view

Parameters

None

Description

Use the **habp enable** command to enable HABP for a switch.

Use the **undo habp enable** command to disable HABP for a switch.

By default, HABP is enabled on a switch.

If an 802.1x-enabled switch does not have HABP enabled, it cannot manage the switches attached to it. So, you need to enable HABP on specific switches in a network with 802.1x enabled.

Examples

Enable HABP.

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

habp server vlan

Syntax

habp server vlan *vlan-id*

undo habp server

View

System view

Parameters

vlan-id: VLAN ID, ranging from 1 to 4094.

Description

Use the **habp server vlan** command to configure a switch to operate as an HABP server. This command also specifies the VLAN where HABP packets are broadcast.

Use the **undo habp server vlan** command to revert to the default HABP mode.

By default, a switch operates as an HABP client.

To specify a switch to operate as an HABP server, you need to enable HABP (using the **habp enable** command) for the switch first. When HABP is not enabled, the **habp server vlan** command cannot take effect.

Examples

Specify the switch to operate as an HABP server and the HABP packets to be broadcast in VLAN 2. (Assume that HABP is enabled.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] habp server vlan 2
```

habp timer

Syntax

habp timer *interval*

undo habp timer

View

System view

Parameters

interval: Interval (in seconds) to send HABP request packets. This argument ranges from 5 to 600.

Description

Use the **habp timer** command to set the interval for a switch to send HABP request packets.

Use the **undo habp timer** command to revert to the default interval.

The default interval for a switch to send HABP request packets is 20 seconds.

Use these two commands on switches operating as HABP servers only.

Examples

```
# Configure the switch to send HABP request packets once in every 50 seconds
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] habp timer 50
```

4 System Guard Configuration Commands

System-Guard Configuration Commands

display system-guard attack-record

Syntax

display system-guard attack-record

View

Any view

Parameter

None

Description

Use the **display system-guard attack-record** command to display the record of detected attacks.

Example

Display the record of detected attacks.

```
<Sysname> display system-guard attack-record
 Not found attack
```

display system-guard state

Syntax

display system-guard state

View

Any view

Parameter

None

Description

Use the **display system-guard state** command to display the state of the system-guard feature.

Related command: **system-guard enable**, **system-guard detect-threshold**, and **system-guard timer-interval**.

Example

Display the state of the system-guard feature.

```
<Sysname> display system-guard state
```

```
System-guard Status: Enabled
Detect Threshold: 201
Isolated Time: 20
Attack Number: 0
```

Table 4-1 Description on the fields of the **display system-guard state** command

Field	Description
System-guard Status	The enable/disable status of the system-guard feature
Detect Threshold	The threshold for the number of packets when an attack is detected
Isolated Time	The length of the isolation after an attack is detected
Attack Number	The times of detected attacks

system-guard detect-threshold

Syntax

system-guard detect-threshold *threshold-value*

undo system-guard detect-threshold

View

System view

Parameter

threshold-value: Threshold for the number of packets when an attack is detected, in the range of 200 to 1,000.

Description

Use the **system-guard detect-threshold** command to set the threshold for the number of packets when an attack is detected. When the number of inbound packets of the same type exceeds the threshold, one attack is detected and recorded.

Use the **undo system-guard detect-threshold** command to restore the threshold to the default value.

By default, the threshold is 200.

Related command: **display system-guard state**.

Example

Set the threshold for the number of packets when an attack is detected to 300.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]system-guard detect-threshold 300
```

system-guard enable

Syntax

system-guard enable

undo system-guard enable

View

System view

Parameter

None

Description

Use the **system-guard enable** command to enable the system-guard feature.

Use the **undo system-guard enable** command to disable the system-guard feature.

By default, the system-guard feature is disabled.

Related command: **display system-guard state**.

Example

Enable the system-guard feature.

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

system-guard timer-interval

Syntax

system-guard timer-interval *isolate-timer*

undo system-guard timer-interval

View

System view

Parameter

isolate-timer: Length of the isolation after an attack is detected, in the range of 1 to 10,000 in minutes.

Description

Use the **system-guard timer-interval** command to set the length of the isolation after an attack is detected.

Use the **undo system-guard timer-interval** command to restore the length of the isolation to the default value.

By default, the length of the isolation after an attack is detected is 10 minutes.

Related command: **display system-guard state**.

Example

Set the length of the isolation after an attack is detected to 20 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]system-guard timer-interval 20
```

Table of Contents

1 AAA Configuration Commands

Note

The maximum length of a domain name is changed from 24 characters to 128 characters. See domain.

AAA Configuration Commands

access-limit

Syntax

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

View

ISP domain view

Parameters

disable: Specifies not to limit the number of access users that can be contained in current ISP domain.

enable *max-user-number*: Specifies the maximum number of access users that can be contained in current ISP domain. The *max-user-number* argument ranges from 1 to 2,072.

Description

Use the **access-limit** command to set the maximum number of access users that can be contained in current ISP domain.

Use the **undo access-limit** command to restore the default setting.

By default, there is no limit on the number of access users in an ISP domain.

Because resource contention may occur among access users, there is a need to limit the number of access users in an ISP domain so as to provide reliable performance to the current users in the ISP domain.

Examples

Allow ISP domain aabbcc.net to contain at most 500 access users.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] access-limit enable 500
```

accounting

Syntax

accounting { **none** | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* }

undo accounting

View

ISP domain view

Parameters

none: Specifies not to perform user accounting.

radius-scheme *radius-scheme-name*: Specifies to use a RADIUS accounting scheme. Here, *radius-scheme-name* is the name of a RADIUS scheme; it is a string of up to 32 characters.

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies to use an HWTACACS accounting scheme. Here, *hwtacacs-scheme-name* is the name of an HWTACACS scheme; it is a string of up to 32 characters.

Description

Use the **accounting** command to configure an accounting scheme for current ISP domain.

Use the **undo accounting** command to cancel the accounting scheme configuration for current ISP domain.

By default, no separate accounting scheme is configured for an ISP domain.

When you use the **accounting** command to reference a RADIUS or HWTACACS scheme in current ISP domain, the RADIUS or HWTACACS scheme must already exist.

The **accounting** command takes precedence over the **scheme** command. If the **accounting** command is used in ISP domain view, the system uses the scheme referenced in the **accounting** command to charge the users in the domain. Otherwise, the system uses the scheme referenced in the **scheme** command to charge the users.

Related commands: **scheme**, **radius scheme**, **hwtacacs scheme**, **accounting optional**.

Examples

Specify "radius" as the RADIUS accounting scheme that will be referenced by ISP domain "aabbcc.net".

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] accounting radius-scheme radius
```

accounting optional

Syntax

accounting optional

undo accounting optional

View

ISP domain view

Parameters

None

Description

Use the **accounting optional** command to open the accounting-optional switch.

Use the **undo accounting optional** command to close the accounting-optional switch so that the system performs accounting for users unconditionally.

By default, the system performs accounting for users unconditionally..

Note that:

- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for an online user, it will not disconnect the user as long as the **accounting optional** command has been executed.
- The **accounting optional** command is commonly used in the cases where only authentication is needed and accounting is not needed.
- If you configure the **accounting optional** command in ISP domain view, it is effective to all users in the domain; if you configure it in RADIUS scheme view, it is effective to users the RADIUS scheme is used for.

Examples

Open the accounting-optional switch for the ISP domain named aabbcc.net.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] accounting optional
```

attribute

Syntax

attribute { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*

undo attribute { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

View

Local user view

Parameters

ip *ip-address*: Sets the IP address of the user.

mac *mac-address*: Sets the MAC address of the user. Here, *mac-address* is in H-H-H format.

idle-cut *second*: Enables the idle-cut function for the local user and sets the allowed idle time. Here, *second* is the allowed idle time, which ranges from 60 to 7,200 seconds.

access-limit *max-user-number*: Sets the maximum number of users who can access the switch with the current username. Here, *max-user-number* ranges from 1 to 1,024.

vlan *vlan-id*: Sets the VLAN attribute of the user (that is, specifies to which VLAN the user belongs). Here, *vlan-id* is an integer ranging from 1 to 4094.

location: Sets the port binding attribute of the user.

nas-ip *ip-address*: Sets the IP address of an access server, so that the user can be bound to a port on the server. Here, *ip-address* is in dotted decimal notation and is 127.0.0.1 by default (representing this device). When binding the user to a remote port, you must use **nas-ip** *ip-address* to specify a remote access server IP address. When binding the user to a local port, you need not use **nas-ip** *ip-address*.

port *port-number*: Sets the port to which you want to bind the user. Here, *port-number* is in the format of device ID/slot number/port number; the device ID ranges from 1 to 8, the slot number ranges from 0 to 15 (if the bound port has no slot number, just input 0 for this item) and the port number ranges from 1 to 255.

Description

Use the **attribute** command to set the attributes of a user whose service type is lan-access.

Use the **undo attribute** command to cancel attribute settings of the user.

You may use **display local-user** command to view the settings of the attributes.

Examples

Create local user user1 and set the IP address attribute of user1 to 10.110.50.1, allowing only the user using the IP address of 10.110.50.1 to use the account user1 for authentication.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
New local user added.
[Sysname-luser- user1] password simple pass1
[Sysname-luser- user1] service-type lan-access
[Sysname-luser-user1] attribute ip 10.110.50.1
```

authentication

Syntax

authentication { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }

undo authentication

View

ISP domain view

Parameters

radius-scheme *radius-scheme-name*: Specifies to use a RADIUS authentication scheme. Here, *radius-scheme-name* is a string of up to 32 characters.

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies to use an HWTACACS authentication scheme. Here, *hwtacacs-scheme-name* is a string of up to 32 characters.

local: Specifies to use local authentication scheme.

none: Specifies not to perform authentication.

Description

Use the **authentication** command to configure an authentication scheme for current ISP domain.

Use the **undo authentication** command to restore the default authentication scheme setting of current ISP domain.

By default, no separate authentication scheme is configured for an ISP domain.

Note that:

- Before you can use the **authentication** command to reference a RADIUS scheme in current ISP domain, the RADIUS scheme must already exist.
- If you execute the **authentication radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary authentication scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, no local authentication will be performed; otherwise, local authentication will be performed.
- If you execute the **authentication hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the local scheme is used as the secondary authentication scheme in case no TACACS server is available. That is, if the communication between the switch and a TACACS server is normal, no local authentication will be performed; otherwise, local authentication will be performed.
- If you execute the **authentication local** command, the local scheme is used as the primary scheme. In this case, there is no secondary authentication scheme.
- If you execute the **authentication none** command, no authentication will be performed.
- The **authentication** command takes precedence over the **scheme** command. If the **authentication** command is configured in an ISP domain view, the system uses the authentication scheme referenced in the command to authenticate the users in the domain; otherwise it uses the scheme referenced in the **scheme** command to authenticate the users.

Related commands: **scheme**, **radius scheme**, **hwtacacs scheme**.

Examples

Reference the RADIUS scheme "radius1" as the authentication scheme of the ISP domain aabbcc.net.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] authentication radius-scheme radius1
```

Reference the RADIUS scheme "rd" as the authentication scheme and the local scheme as the secondary authentication scheme of the ISP domain aabbcc.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc
New Domain added.
[Sysname-isp-aabbcc] authentication radius-scheme rd local
```

authentication super

Syntax

authentication super hwtacacs-scheme *hwtacacs-scheme-name*

undo authentication super

View

ISP domain view

Parameters

hwtacacs-scheme-name: Name of the HWTACACS authentication scheme, a string of 1 to 32 characters.

Description

Use the **authentication super** command to specify a HWTACACS authentication scheme for user level switching in the current ISP domain.

Use the **undo authentication super** command to remove the specified HWTACACS authentication scheme.

By default, no HWTACACS authentication scheme is configured for user level switching.

When you execute the **authentication super** command to specify a HWTACACS authentication scheme for user level switching, the HWTACACS scheme must exist.

Note

The Switch 4200G adopts hierarchical protection for command lines so as to inhibit users at lower levels from using higher level commands to configure the switches. For details about configuring a HWTACACS authentication scheme for low-to-high user level switching, refer to *Switching User Level* in the *Command Line Interface Operation*.

Related commands: **hwtacacs scheme**.

Examples

Set the HWTACACS scheme to **ht** for user level switching in the current ISP domain aabbcc.net.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] authentication super hwtacacs-scheme ht
```

authorization

Syntax

authorization { **none** | **hwtacacs-scheme** *hwtacacs-scheme-name* }

undo authorization

View

ISP domain view

Parameters

none: Specifies not to use any authorization scheme.

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies to use an HWTACACS scheme. Here, *hwtacacs-scheme-name* is the name of an HWTACACS scheme; it is a string of up to 32 characters.

Description

Use the **authorization** command to configure an authorization scheme for current ISP domain.

Use the **undo authorization** command to restore the default authorization scheme setting of the ISP domain.

By default, no separate authorization scheme is configured for an ISP domain.

Related commands: **scheme**, **radius scheme**, **hwtacacs scheme**.

Examples

Allow users in ISP domain aabbcc.net to access network services without being authorized.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] authorization none
```

authorization vlan

Syntax

authorization vlan *string*

undo authorization vlan

View

Local user view

Parameters

string: Number or descriptor of the authorized VLAN for the current user, a string of 1 to 32 characters. If it is a numeral string and there is a VLAN with the number configured, it specifies the VLAN. If it is a numeral string but no VLAN is present with the number, it specifies the VLAN using it as the VLAN descriptor.

Description

Use the **authorization vlan** command to specify an authorized VLAN for a local user. A user passing the authentication of the local RADIUS server can access network resources in the authorized VLAN.

Use the **undo authorization vlan** command to remove the configuration.

By default, no authorized VLAN is specified for a local user.

Note

For local **RADIUS** authentication to take effect, the VLAN assignment mode must be set to **string** after you specify authorized VLANs for local users.

Examples

Specify the authorized VLAN for local user 00-14-22-2C-AA-69 as VLAN 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user 00-14-22-2C-AA-69
[Sysname-luser-00-14-22-2C-AA-69] authorization vlan 2
```

cut connection

Syntax

cut connection { **all** | **access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }

View

System view

Parameters

all: Cuts down all user connections.

access-type { **dot1x** | **mac-authentication** }: Cuts down user connections of a specified access type. **dot1x** is used to cut down all 802.1x user connections, and **mac-authentication** is used to cut down all MAC authentication user connections.

domain *isp-name*: Cuts down all user connections in a specified ISP domain. Here, *isp-name* is the name of an ISP domain, a string of up to 128 characters. You can only specify an existing ISP domain.

interface *interface-type interface-number*: Cuts down all user connections under a specified port. Here, *interface-type* is a port type and *interface-number* is a port number.

ip *ip-address*: Cuts down all user connections with a specified IP address.

mac *mac-address*: Cuts down the user connection with a specified MAC address. Here, *mac-address* is in H-H-H format.

radius-scheme *radius-scheme-name*: Cuts down all user connections using a specified RADIUS scheme. Here, *radius-scheme-name* is a string of up to 32 characters.

vlan *vlan-id*: Cuts down all user connections of a specified VLAN. Here, *vlan-id* ranges from 1 to 4094.

ucibindex *ucib-index*: Cuts down the user connection with a specified connection index. Here, *ucib-index* ranges from 0 to 1047.

user-name *user-name*: Cuts down the connection of a specified user. Here, *user-name* is a string of up to 184 characters..

Description

Use the **cut connection** command to forcibly cut down one user connection, one type of user connections, or all user connections.

This command cannot cut down the connections of Telnet and FTP users.

Related commands: **display connection**.

Examples

Cut down all user connections under the ISP domain aabbcc.net.

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

display connection

Syntax

display connection [**access-type** { **dot1x | mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]

View

Any view

Parameters

access-type { **dot1x** | **mac-authentication** }: Displays user connections of a specified access type. Here, **dot1x** is used to display all 802.1x user connections, and **mac-authentication** is used to display all MAC authentication user connections.

domain *isp-name*: Displays all user connections under specified ISP domain. Here, *isp-name* is the name of an ISP domain, a string of up to 128 characters. You can only specify an existing ISP domain.

interface *interface-type interface-number*: Displays all user connections on a specified port.

ip *ip-address*: Displays all user connections with a specified IP address.

mac *mac-address*: Displays the user connection with a specified MAC address. Here, *mac-address* is in hexadecimal format (in the form of H-H-H).

radius-scheme *radius-scheme-name*: Displays all user connections using a specified RADIUS scheme. Here, *radius-scheme-name* is a string of up to 32 characters.

hwtacacs-scheme *hwtacacs-scheme-name*: Displays all user connections using a specified RADIUS scheme. Here, *hwtacacs-scheme-name* is a string of up to 32 characters.

vlan *vlan-id*: Displays all user connections of a specified VLAN. Here, *vlan-id* ranges from 1 to 4094.

ucibindex *ucib-index*: Displays the user connection with a specified connection index. Here, *ucib-index* ranges from 0 to 1047.

user-name *user-name*: Displays the connection of a specified user. Here, *user-name* is a character string in the format of pure-username@domain-name. The pure-username cannot be longer than 55 characters, the domain-name cannot be longer than 24 characters, and the entire user-name cannot be longer than 184 characters.

Description

Use the **display connection** command to display information about specified or all user connections.

If you execute this command without specifying any parameter, all user connections will be displayed.

This command cannot display information about the connections of FTP users.

Related commands: **cut connection**.

Examples

Display information about all user connections.

```
<Sysname> display connection
------------------unit 1-----------------------
Index=40 , Username=user1@domain1
MAC=000f-3d80-4ce5  , IP=0.0.0.0
 On Unit 1: Total 1 connections matched, 1 listed.
```

Display information about the user connection with index 0.

```
[Sysname] display connection ucibindex 0
Index=0   , Username=user1@system
MAC=000f-3d80-4ce5   , IP=192.168.0.3
Access=8021X   ,Auth=CHAP    ,Port=Ether   ,Port NO=0x10003001
Initial VLAN=1, Authorization VLAN=1
ACL Group=Disable
CAR=Disable
Priority=Disable
Start=2000-04-03 02:51:53 ,Current=2000-04-03 02:52:22 ,Online=00h00m29s
 On Unit 1:Total 1 connections matched, 1 listed.
 Total 1 connections matched, 1 listed.
```

Here, Port NO=0x10003001 means (by the binary bits):

Table 1-1 Description of the Port NO field

31 to 28 bit	27 to 24 bit	23 to 20 bit	19 to 12 bit	11 to 0 bit
UNIT ID	Slot number	Sub-slot number	Port number	VLAN ID

display domain

Syntax

display domain [*isp-name*]

View

Any view

Parameters

isp-name: Name of an ISP domain, a string of up to 128 characters. This must be the name of an existing ISP domain.

Description

Use the **display domain** command to display configuration information about one specific or all ISP domains.

Related commands: **access-limit**, **domain**, **scheme**, **state**.

Examples

Display configuration information about all ISP domains.

```
<Sysname> display domain
0  Domain = system
   State = Active
   Scheme = LOCAL
   Access-limit = 512
   Vlan-assignment-mode = Integer
   Domain User Template:
   Idle-cut = = Enable Time = 60(min) Flow = 200(byte)
   Self-service URL = http://aabbcc.net
   Messenger Time Maxlimit = 30(min) span = 10(min)

Default Domain Name: system
Total 1 domain(s).1 listed.
```

Table 1-2 Description on the fields of the **display domain** command

Field	Description
Domain	Domain name
State	Status of the domain, which can be **active** or **block**.
Scheme	AAA scheme that the domain uses
Access-Limit	Maximum number of local user connections in the domain
Vlan-assignment-mode	VLAN assignment mode, which can be Integer or String.
Domain User Template	Domain user template settings, that is, attribute settings for all users in the domain.
Idle-Cut	Status of the idle-cut function
Self-service URL	Self-service URL for password changing
Messenger Time	Settings of the messenger time service, which is for reminding online users of their remaining online time. The setting in this example indicates that the system starts to remind an online user (at an interval of 10 minutes) when the remaining online time is 30 minutes.
Default Domain Name	Default ISP domain of the system

display local-user

Syntax

display local-user [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **vlan** *vlan-id* | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name*]

View

Any view

Parameters

domain *isp-name*: Displays all local users belonging to a specified ISP domain. Here, *isp-name* is the name of an ISP domain, a string of up to 128 characters. You can only specify an existing ISP domain.

idle-cut { **disable** | **enable** }: Displays the local users who are inhibited from enabling the idle-cut function, or the local users who are allowed to enable the idle-cut function. Here, **disable** specifies the inhibited local users and **enable** specifies the allowed local users.

vlan *vlan-id*: Displays the local users belonging to a specified VLAN. Here, *vlan-id* ranges from 1 to 4094.

service-type: Displays the local users of a specified type. You can specify one of the following user types: **ftp**, **lan-access** (generally, this type of users are Ethernet access users, for example, 802.1x users), **ssh**, **telnet**, and **terminal** (this type of user is a terminal user who logs into the switch through the Console port).

state { **active** | **block** }: Displays the local users in a specified state. Here **active** represents the users allowed to request network services, and **block** represents the users inhibited from requesting network services.

user-name *user-name*: Displays the local user with a specified username. Here, *user-name* is a string of up to 184 characters.

Description

Use the **display local-user** command to display information about specified or all local users.

Related commands: **local-user**.

Examples

Display information about all local users.

```
<Sysname> display local-user
0  The contents of local user test:
   State:                   Active          ServiceType Mask: L
   Idle-cut:                Enable          Idle TimeOut: 3600 seconds
   Access-limit:            Enable          Current AccessNum: 1
   Max AccessNum:           1024
   Bind location:           127.0.0.1/1/0/2 (NAS/UNITID/SUBSLOT/PORT)
   Vlan ID:                 1
   Authorization VLAN:      2
   IP address:              192.168.0.108
   MAC address:             000d-88f6-44c1
Total 1 local user(s) Matched, 1 listed.
ServiceType Mask Meaning: C--Terminal  F--FTP  L--LanAccess  S--SSH  T--Telnet
```

Table 1-3 describes the fields in the above display output.

Table 1-3 Description on the fields of the **display local-user** command

Field	Description
State	Status of the local user
ServiceType Mask	Service type mask: T means Telnet service. S means SSH service. C means client service. LM means lan-access service. F means FTP service. None means no defined service.
Idle-cut	Status of the idle-cut function
Access-limit	Limit on the number of access users
Current AccessNum	Number of current access users
Bind location	Whether or not bound to a port
Vlan ID	VLAN of the user
Authorization VLAN	Authorized VLAN of the user
IP address	IP address of the user
MAC address	MAC address of the user

domain

Syntax

domain { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

View

System view

Parameters

isp-name: Name of an ISP domain, a string of up to 128 characters. This string cannot contain the following characters: /\:*?<>|. If the domain name includes one or more “~” characters and the last “~” is followed by numerals, it must be followed by at least five numerals to avoid confusion. This is because any domain name longer than 16 characters will appear in the form of “system prompt-the first 15 characters of the domain name~4-digit index” in the view prompt to avoid word wrap.

default: Manually changes the default ISP domain, which is "system" by default. There is one and only one default ISP domain.

disable: Disables the configured default ISP domain.

enable: Enables the configured default ISP domain.

Description

Use the **domain** command to create an ISP domain and enter its view, or enter the view of an existing ISP domain, or configure the default ISP domain.

Use the **undo domain** command to delete a specified ISP domain.

The ISP domain "system" is used as the default ISP domain before you manually configure the default ISP domain, and you can use the **display domain** command to check the settings of the default ISP domain "system".

After you execute the **domain** command, the system creates a new ISP domain if the specified ISP domain does not exist. Once an ISP domain is created, it is in the **active** state. You can manually specify an ISP domain as the default domain only when the specified domain already exists.

Related commands: **access-limit**, **scheme**, **state**, **display domain**.

Examples

Create a new ISP domain named aabbcc.net.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net]
```

Create a new ISP domain named 01234567891234567 (note that it will appear as 012345678912345~0001 in the view prompt).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]domain 01234567891234567
New Domain added.
[Sysname-isp-012345678912345~0001]
```

domain delimiter

Syntax

domain delimiter { **at** | **dot** }

undo domain delimiter

View

System view

Parameters

at: Specifies “@” as the delimiter between the username and the ISP domain name.

dot: Specifies “.” as the delimiter between the username and the ISP domain name.

Description

Use the **domain delimiter** command to specify the delimiter form between the username and the ISP domain name.

Use the **undo domain delimiter** command to restore the delimiter form to the default setting.

By default, the“@” character is used as the delimiter between the username and the ISP domain name.

Note

- If you have configured to use "." as the delimiter, for a username that contains multiple ".", the first "." will be used as the domain delimiter.
- If you have configured to use "@" as the delimiter, the "@" must not appear more than once in the username. If “.” is the delimiter, the username must not contain any “@”.

Related commands: **domain**.

Examples

Specify “.” as the delimiter between the username and the ISP domain name.

```
<Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[Sysname] domain delimiter dot
```

idle-cut

Syntax

idle-cut { **disable** | **enable** *minute flow* }

View

ISP domain view

Parameters

disable: Disables the idle-cut function for the domain.

enable: Enables the idle-cut function for the domain.

minute: Maximum idle time in minutes, ranging from 1 to 120.

flow: Minimum traffic in bytes, ranging from 1 to 10,240,000.

Description

Use the **idle-cut** command to set the user idle-cut function in current ISP domain. If a user’s traffic in the specified period of time is less than the specified amount, the system will disconnect the user.

By default, this function is disabled.

Note that if the authentication server assigns the idle-cut settings, the assigned ones take precedence over the settings configured here.

Related commands: **domain**.

Examples

Enable the idle-cut function for ISP domain aabbcc.net, setting the maximum idle time to 50 minutes and the minimum traffic to 500 bytes. After this configuration, if a user in the domain has no traffic or has less than 500 bytes of traffic within 50 minutes, the system will tear down the user's connection.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] idle-cut enable 50 500
```

level

Syntax

level *level*

undo level

View

Local user view

Parameters

level: Privilege level to be set for the user. It is an integer ranging from 0 to 3.

Description

Use the **level** command to set the privilege level of the user. The privilege level of the user corresponds to the command level of the user. For detailed information, refer to the description of the **command-privilege level** command in the *command line interface* part.

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

The default privilege level is 0.

Note that:

- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.
- If the configured authentication method requires a username and a password, the command level that a user can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels sets on their user interfaces.

Related commands: **local-user**.

Examples

Set the level of user1 to 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1] level 3
```

local-user

Syntax

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** }] }

View

System view

Parameters

user-name: Local username, a string of up to 184 characters. This string cannot contain the following characters: /:*?<>. It can contain no more than one @ character. The pure username (user ID, that is, the part before @) cannot be longer than 55 characters, and the domain name (the part behind @) cannot be longer than 128 characters. If the username includes one or more “~” characters and the last “~” is followed by numerals, it must be followed by at least five numerals to avoid confusion. This is because any username longer than 16 characters will appear in the form of “system prompt-the first 15 characters of the username~4-digit index” in the view prompt to avoid word wrap.

all: Specifies all local users.

service-type: Specifies the local users of a specified type. You can specify one of the following user types: **ftp**, **lan-access** (generally, this type of users are Ethernet access users, for example, 802.1x users), **ssh**, **telnet**, and **terminal** (terminal user who logs into the switch through the Console port).

Description

Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to delete one or more local users of the specified type.

By default, there is no local user in the system.

Related commands: **display local-user**, **service-type**.

Examples

Add a local user named user1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1]
```

Add a local user named 01234567891234567 (note that it will appear as 012345678912345~0000 in the view prompt).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]local-user 01234567891234567
New local user added.
[Sysname-luser-012345678912345~0000]
```

local-user password-display-mode

Syntax

local-user password-display-mode { **cipher-force | auto** }

undo local-user password-display-mode

View

System view

Parameters

cipher-force: Adopts the forcible cipher mode so that all local users' the passwords will be displayed in cipher text.

auto: Adopts the automatic mode so that each local user's password will be displayed in the mode you have set for the user by the **password** command.

Description

Use the **local-user password-display-mode** command to set the password display mode of all local users.

Use the **undo local-user password-display-mode** command to restore the default password display mode of all local users.

By default, the password display mode of all access users is **auto**.

If the **cipher-force** mode is adopted, all passwords will be displayed in cipher text even though you have specified to display some users passwords in plain text by using the **password** command with the **simple** keyword.

Related commands: **display local-user**, **password**.

Examples

Specify to display all local user passwords in cipher text in whatever cases.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user password-display-mode cipher-force
```

messenger

Syntax

messenger time { **enable** *limit interval* | **disable** }

undo messenger time

View

ISP domain view

Parameters

limit: Time limit in minutes, ranging from 1 to 60. The switch will send prompt messages at regular intervals to users whose remaining online time is less than this limit.

interval: Interval to send prompt messages (in minutes). This argument ranges from 5 to 60 and must be a multiple of 5.

Description

Use the **messenger time enable** command to enable the messenger function and set the related parameters.

Use the **messenger time disable** command to disable the messenger function.

Use the **undo messenger time** command to restore the messenger function to its default state.

By default, the messenger function is disabled on the switch.

The purpose of this function is to remind online users of their remaining online time through clients by message dialog box.

Examples

Enable the switch to send prompt messages at intervals of 5 minutes to the users in the ISP domain "system" after their remaining online time is less than 30 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain system
[Sysname-isp-system] messenger time enable 30 5
```

name

Syntax

name *string*

undo name

View

VLAN view

Parameters

string: Assigned VLAN name, a string of up to 32 characters.

Description

Use the **name** command to set a VLAN name, which will be used for VLAN assignment.

Use the **undo name** command to cancel the VLAN name.

By default, a VLAN uses its VLAN ID (like VLAN 0001) as its assigned VLAN name.

This command is used in conjunction with the dynamic VLAN assignment function. For details about dynamic VLAN assignment, refer to the **vlan-assignment-mode** command.

Related commands: **vlan-assignment-mode**.

Examples

Set the name of VLAN 100 to **test**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 100
```

```
[Sysname-vlan100] name test
```

password

Syntax

password { **simple** | **cipher** } *password*

undo password

View

Local user view

Parameters

simple: Specifies the password in plain text.

cipher: Specifies the password in cipher text.

password: Password to be set:

- For **simple** mode, the password you input must be a plain-text password.
- For **cipher** mode, the password can be either a cipher-text password or a plain-text password, and what it is depends on your input.

A password in plain text can be a string of up to 63 consecutive characters, for example, aabbcc. A password in cipher text can be a string of 24 or 88 characters, for example, (TT8F]Y\5SQ=^Q`MAF4<1!!.

Description

Use the **password** command to set a password for the local user.

Use the **undo password** command to cancel the password of the local user.

Note that:

- With the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the password command.
- With the **cipher** keyword specified, a password of up to 16 characters in plain text will be encrypted into a password of 24 characters in cipher text, and a password of 16 to 63 characters in plain text will be encrypted into a password of 88 characters in cipher text. For a password of 24 characters, if the system can decrypt the password, the system treats it as a password in cipher text. Otherwise, the system treats it as a password in plain text.

Related commands: **display local-user**.

Examples

Set the password of user1 to 20030422 and specify to display the password in plain text.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1] password simple 20030422
```

radius-scheme

Syntax

radius-scheme *radius-scheme-name*

View

ISP domain view

Parameters

radius-scheme-name: Name of a RADIUS scheme, a string of up to 32 characters.

Description

Use the **radius-scheme** command to configure a RADIUS scheme for current ISP domain.

After an ISP domain is initially created, it uses the local AAA scheme instead of any RADIUS scheme by default.

The RADIUS scheme you specified in the **radius-scheme** command must already exist. This command is equivalent to the **scheme radius-scheme** command.

Related commands: **radius scheme**, **scheme**, **display radius scheme**.

Examples

Configure the ISP domain "aabbcc.net" to use the RADIUS scheme "extended".

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] radius-scheme extended
```

scheme

Syntax

scheme { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }

undo scheme [**none** | **radius-scheme** | **hwtacacs-scheme**]

View

ISP domain view

Parameters

radius-scheme-name: Name of a RADIUS scheme, a string of up to 32 characters.

hwtacacs-scheme-name: Name of a HWTACACS scheme, a string of up to 32 characters.

local: Specifies to use local authentication.

none: Specifies not to perform authentication.

Description

Use the **scheme** command to configure an AAA scheme for current ISP domain.

Use the **undo scheme** command to restore the default AAA scheme configuration for the ISP domain.

By default, the ISP domain uses the **local** AAA scheme.

Note that:

- When you execute the **scheme** command to reference a RADIUS scheme in current ISP domain, the referenced RADIUS scheme must already exist.
- If you execute the **scheme radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no TACACS server is available. That is, if the communication between the switch and a TACACS server is normal, no local authentication is performed; If the TACACS server is not reachable or there is a key error or NAS IP error, local authentication is performed.
- If you execute the **scheme local** or **scheme none** command to use **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case, no secondary scheme can be specified and therefore no scheme switching will occur.
- Both the **radius-scheme** command and the **scheme** command can be used to specify the RADIUS scheme to be quoted for the ISP domain. Their functions are the same and the system takes the latest configuration.

Related commands: **radius scheme**, **display domain**.

Examples

Configure the ISP domain aabbcc.net to use RADIUS scheme radius1 as the primary AAA scheme and use the local scheme as the secondary authentication scheme.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] scheme radius-scheme raduis1 local
```

self-service-url

Syntax

self-service-url { **disable** | **enable** *url-string* }

undo self-service-url

View

ISP domain view

Parameters

url-string: URL of the web page used to modify user password on the self-service server. It is a string of 1 to 64 characters. This string cannot contain any question mark "?". If the actual URL of the self-service server contains a question mark, you should change it to an elect bar "|".

Description

Use the **self-service-url enable** command to enable the self-service server location function

Use the **self-service-url disable** command to disable the self-service server location function

Use the **undo self-service-url** command to restore the default state of this function.

By default, this function is disabled.

Note that:

- This command must be used with the cooperation of a self-service-supported RADIUS server (such as CAMS). Through self-service, users can manage and control their accounts or card numbers by themselves. A server installed with the self-service software is called a self-service server.
- After this command is executed on the switch, a user can locate the self-service server through the following operation: choose [change user password] on the 802.1x client, the client opens the default browser (for example, IE or Netscape) and locates the URL page used to change user password on the self-service server. Then, the user can change the password.
- A user can choose the [change user password] option on the client only after passing the authentication. If the user fails the authentication, this option is in grey and is unavailable.

Examples

Under the default ISP domain "system", set the URL of the web page used to modify user password on the self-service server to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain system
[Sysname-isp-system]                    self-service-url                    enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

service-type

Syntax

service-type { **ftp** | **lan-access** | { **telnet** | **ssh** | **terminal** }* [**level** *level*] }

undo service-type { **ftp** | **lan-access** | { **telnet** | **ssh** | **terminal** }* }

View

Local user view

Parameters

ftp: Specifies that this is an FTP user.

lan-access: Specifies that this is a LAN access user (who is generally an Ethernet access user, for example, 802.1x user).

telnet: Authorizes the user to access the Telnet service.

ssh: Authorizes the user to access the SSH service.

terminal: Authorizes the user to access the terminal service (that is, allows the user to log into the switch through the Console port).

level *level*: Specifies the level of the Telnet, terminal or SSH user. Here, *level* is an integer ranging from 0 to 3 and defaulting to 0.

Description

Use the **service-type** command to authorize a user to access one or more types of services.

Use the **undo service-type** command to inhibit a user from accessing specified types of services.

By default, a user is inhibited from accessing any type of service.

You may user the **display local-user** command to view the types of services that a user is authorized to access.

Examples

Authorize user1 to access the Telnet service.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1] service-type telnet
```

state

Syntax

state { **active** | **block** }

View

ISP domain view, local user view

Parameters

active: Activates the current ISP domain (in ISP domain view) or local user (in local user view), to allow users in current ISP domain or current local user to access the network.

block: Blocks the current ISP domain (in ISP domain view) or local user (in local user view), to inhibit users in current ISP domain or current local user from accessing the network.

Description

Use the **state** command to set the status of current ISP domain (in ISP domain view) or current local user (in local user view).

By default, an ISP domain/local user is in the **active** state once it is created.

After an ISP domain is set to the **block** state, except for online users, users in this domain are inhibited from accessing the network.

After a local user is set to the **block** state, the user is inhibited from accessing the network unless the user is already online.

Related commands: **domain**, **local-user**.

You may use the **display domain** command or the **display local-user** command to view the status information.

Examples

Set the ISP domain aabbcc.net to the block state, so that all its offline users cannot access the network.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] state block
```

Set user1 to the block state.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user user1
[Sysname-user-user1] state block
```

vlan-assignment-mode

Syntax

vlan-assignment-mode { **integer** | **string** }

View

ISP domain view

Parameters

integer: Sets the VLAN assignment mode to integer.

string: Sets the VLAN assignment mode to string.

Description

Use the **vlan-assignment-mode** command to set the VLAN assignment mode (integer or string) on the switch.

By default, the VLAN assignment mode is integer, that is, the switch supports its RADIUS authentication server to assign integer VLAN IDs.

The dynamic VLAN assignment feature enables a switch to dynamically add the ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

In actual applications, to use this feature together with Guest VLAN, you are recommended to set port control to port-based mode.

Currently, the switch supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS

authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

The switch supports two dynamic VLAN assignment modes to adapt to different authentication servers. You are recommended to configure the switch according to the dynamic VLAN assignment mode used by the server.

Table 1-4 lists several commonly used RADIUS servers and their dynamic VLAN assignment modes.

Table 1-4 Commonly used servers and their dynamic VLAN assignment modes

Server	Dynamic VLAN assignment mode
CAMS	Integer For the latest CAMS version, you can determine the assignment mode by attribute value.
ACS	String
FreeRADIUS	You can determine the assignment mode by attribute value (for example, 100 is integer; “100” is string).
Shiva Access Manager	String
Steel-Belted Radius Administrator	String

Note

In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the value as the VLAN ID (VLAN 1024, for example).

Related commands: **name**.

Examples

Set the VLAN assignment mode of the domain aabbcc.net to **string**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] vlan-assignment-mode string
```

RADIUS Configuration Commands

accounting optional

Syntax

accounting optional

undo accounting optional

View

RADIUS scheme view

Parameters

None

Description

Use the **accounting optional** command to open the accounting-optional switch.

Use the **undo accounting optional** command to close the accounting-optional switch so that the system performs accounting for users unconditionally.

By default, the system performs accounting for users unconditionally.

Note that:

- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for an online user, it will not disconnect the user as long as the **accounting optional** command has been executed. This command is commonly used in the cases where only authentication is needed and accounting is not needed.
- This configuration takes effect only on the ISP domains using this RADIUS scheme.
- If you configure the **accounting optional** command in ISP domain view, it is effective to all users in the domain; if you configure it in RADIUS scheme view, it is effective to users the RADIUS scheme is used for.

Examples

Open the accounting-optional switch in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] accounting optional
```

accounting-on enable

Syntax

accounting-on enable [**send** *times* | **interval** *interval*]

undo accounting-on { **enable** | **send** | **interval** }

View

RADIUS scheme view

Parameters

times: Maximum number of attempts to send an Accounting-On message, ranging from 1 to 256 and defaulting to 15. If the maximum number has been reached but the switch still receives no response from the CAMS, the switch stops sending Accounting-On messages.

interval: Interval to send Accounting-On messages (in seconds), ranging from 1 to 30 and defaulting to 3.

Description

Use the **accounting-on enable** command to enable the user re-authentication at restart function.

Use the **undo accounting-on enable** command to disable the user re-authentication at restart function and restore the default interval and maximum number of attempts to send Accounting-On messages.

Use the **undo accounting-on send** command to restore the default maximum number of attempts to send Accounting-On messages.

Use the **undo accounting-on interval** command to restore the default interval to send Accounting-On messages.

By default, the user re-authentication at restart function is disabled.

The purpose of this function is to solve this problem: users cannot re-log into the switch after the switch restarts because they are regarded as already online. After this function is enabled, every time the switch restarts, it sends an Accounting-On message to the RADIUS server to tell the server that it has restarted and ask the server to log out its users. The following gives the operations after the switch restarts:

1) The switch generates an Accounting-On message, which mainly contains the following information: NAS-ID, NAS-IP-address (source IP address), and session ID. You can configure the NAS-IP-address argument manually by using the **nas-ip** command. When configuring the NAS-IP-address argument, be sure to specify an appropriate valid IP address. If you do not configure the NAS-IP-address argument, the switch automatically uses the IP address of a VLAN interface as the NAS-IP-address.
2) The switch sends the Accounting-On message to the CAMS at regular intervals.
3) Once the CAMS receives the Accounting-On message, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who were accessing the network through the switch before the restart according to the information (NAS-ID, NAS-IP-address and session ID) contained in the message, and ends the accounting of the users based on the last accounting update message.
4) Once the switch receives the response from the CAMS, it stops sending Accounting-On messages.
5) If the switch does not receive any response from the CAMS after it has tried the configured maximum number of times to send the Accounting-On message, it will not send the Accounting-On message any more.

Note

- After configuring the **accounting-on enable** command, you need to execute the **save** command so that the command can take effect when the switch restarts.
- This function requires the cooperation of the H3C CAMS system.

Related commands: **nas-ip**.

Examples

Enable the user re-authentication at restart function for the RADIUS scheme named radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable
```

calling-station-id mode

Syntax

calling-station-id mode { **mode1 | mode2** } { **lowercase | uppercase** }

undo calling-station-id mode

View

RADIUS scheme view

Parameters

mode1: Sets the MAC address format to XXXX-XXXX-XXXX, where each X represents a hexadecimal number.

mode2: Sets the MAC address format to XX-XX-XX-XX-XX-XX.

lowercase: Uses lowercase letters in the MAC address.

uppercase: Uses uppercase letters in the MAC address.

Description

Use the **calling-station-id mode** command to configure the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets.

Use the **undo calling-station-id mode** command to restore the default format.

By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase.

Examples

Set the MAC address format of the Calling-Station-Id field to **XX-XX-XX-XX-XX-XX**, in uppercase.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]radius scheme system
[Sysname-radius-system]calling-station-id mode mode2 uppercase
```

data-flow-format

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

View

RADIUS scheme view

Parameters

data: Sets the data unit of outgoing RADIUS flows, which can be byte, giga-byte, kilo-byte, or mega-byte.

packet: Sets the packet unit of outgoing RADIUS flows, which can be one-packet, giga-packet, kilo-packet, or mega-packet.

Description

Use the **data-flow-format** command to set the units of RADIUS data flows to RADIUS servers.

Use the **undo data-flow-format** command to restore the default units.

By default, the data unit and packet unit of outgoing RADIUS flows are byte and one-packet respectively.

Note that the specified unit of data flows sent to the RADIUS server must be consistent with the traffic statistics unit of the RADIUS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display radius scheme**.

Examples

Specify to measure data and packets in data flows to RADIUS servers in kilo-bytes and kilo-packets respectively in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display local-server statistics

Syntax

display local-server statistics

View

Any view

Parameters

None

Description

Use the **display local-server statistics** command to display the RADIUS message statistics about local RADIUS server.

Related commands: **local-server**.

Examples

Display the RADIUS message statistics about local RADIUS server.

```
<Sysname> display local-server statistics
On Unit 1:
The localserver packet statistics:
Receive:                  30         Send:                    30
Discard:                  0          Receive Packet Error:    0
Auth Receive:             10         Auth Send:                10
Acct Receive:             20         Acct Send:                20
```

display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

View

Any view

Parameters

radius-scheme-name: Name of a RADIUS scheme, a string of up to 32 characters.

Description

Use the **display radius scheme** command to display configuration information about one specific or all RADIUS schemes

Related commands: **radius scheme**.

Examples

Display configuration information about all RADIUS schemes.

```
<Sysname> display radius scheme
------------------------------------------------------------------
SchemeName  =system                           Index=0    Type=extended
Primary Auth IP  =127.0.0.1        Port=1645
Primary Acct IP  =127.0.0.1        Port=1646
Second  Auth IP  =0.0.0.0          Port=1812
Second  Acct IP  =0.0.0.0          Port=1813
Auth Server Encryption Key= Not configured
Acct Server Encryption Key= Not configured
Accounting method = required
Accounting-On packet enable, send times = 15 , interval = 3s
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
```

```
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min)                             =5
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =1
calling_station_id format                           =XXXX-XXXX-XXXX in lowercase
unit 1 :
Primary Auth State=active,   Second Auth State=block
Primary Acc  State=active,   Second Acc  State=block


-----------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

Table 1-5 Description on the fields of the **display radius scheme** command

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS servers
Primary Auth IP/Port	IP address/port number of the primary authentication server
Primary Acct IP/Port	IP address/port number of the primary accounting server
Second Auth IP/Port	IP address/port number of the secondary authentication server
Second Acct IP/Port	IP address/port number of the secondary accounting server
Auth Server Encryption Key	Shared key for the authentication servers
Acct Server Encryption Key	Shared key for the accounting servers
Accounting method	Accounting method
Accounting-On packet enable, send times = 15 , interval = 3s	The switch sends up to 15 Accounting-On messages at intervals of 3 seconds after restarting.
TimeOutValue(in second)	RADIUS server response timeout time
RetryTimes	Maximum number of transmission attempts of a RADIUS request
RealtimeACCT(in minute)	Real-time accounting interval in minutes
Permitted send realtime PKT failed counts	maximum allowed number of continuous real-time accounting failures
Retry sending times of noresponse acct-stop-PKT	Maximum number of transmission attempts of the buffered stop-accounting requests
Quiet-interval(min)	Time that the switch must wait before it can restore the status of a primary server to active
Username format	Username format
Data flow unit	Data unit of data flow

Field	Description
Packet unit	Packet unit of data flow
calling_station_id format	MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets
Primary Auth State	Status of the primary authentication server
Second Auth State	Status of the secondary authentication server
Primary Acc State	Status of the primary accounting server
Second Acc State	Status of the secondary accounting server

display radius statistics

Syntax

display radius statistics

View

Any view

Parameters

None

Description

Use the **display radius statistics** command to display the RADIUS message statistics.

Related commands: **radius scheme**.

Examples

Display RADIUS message statistics.

```
<Sysname> display radius statistics
state statistic(total=1048):
     DEAD=1048     AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=0
 AcctStop=0          OnLine=0            Stop=0
 StateErr=0

Received and Sent packets statistic:
Unit 1.....................................
Sent PKT total  :0        Received PKT total:0
RADIUS received packets statistic:
Code= 2,Num=0       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=0       ,Err=0
Code=11,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
```

```
Normal auth request             , Num=0       , Err=0       , Succ=0
EAP auth request                , Num=0       , Err=0       , Succ=0
Account request                 , Num=0       , Err=0       , Succ=0
Account off request             , Num=0       , Err=0       , Succ=0
PKT auth timeout                , Num=0       , Err=0       , Succ=0
PKT acct_timeout                , Num=0       , Err=0       , Succ=0
Realtime Account timer          , Num=0       , Err=0       , Succ=0
PKT response                    , Num=0       , Err=0       , Succ=0
EAP reauth_request              , Num=0       , Err=0       , Succ=0
PORTAL access                   , Num=0       , Err=0       , Succ=0
Update ack                      , Num=0       , Err=0       , Succ=0
PORTAL access ack               , Num=0       , Err=0       , Succ=0
Session ctrl pkt                , Num=0       , Err=0       , Succ=0
Set policy result               , Num=0       , Err=0       , Succ=0
RADIUS sent messages statistic:
Auth accept                     , Num=0
Auth reject                     , Num=0
EAP auth replying               , Num=0
Account success                 , Num=0
Account failure                 , Num=0
Cut req                         , Num=0
Set policy result               , 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 =0
Discarded No-response-acct-stop packet for buffer overflow =0
```

display stop-accounting-buffer

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View

Any view

Parameters

radius-scheme *radius-scheme-name*: Displays the buffered stop-accounting requests of a specified RADIUS scheme. Here, *radius-scheme-name* is a string of up to 32 characters.

session-id *session-id*: Displays the buffered stop-accounting requests of a specified session. Here, *session-id* is a string of up to 50 characters.

time-range *start-time stop-time*: Displays the buffered stop-accounting requests generated in a specified time range. Here, *start-time* is the start time of the time range, *stop-time* is the end time of the time range, and both are in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd. The

parameters here are used to display all the buffered stop-accounting requests generated from *start-time* to *stop-time*.

user-name *user-name*: Displays the buffered stop-accounting requests of a specified user. Here, *user-name* is a string of up to 184 characters.

Description

Use the **display stop-accounting-buffer** command to display the non-response stop-accounting requests buffered in the device.

Note

- You can choose to display the buffered stop-accounting requests of a specified RADIUS scheme, session (by session ID), or user (by username). You can also specify a time range to display those generated within the specified time range. The displayed information helps you diagnose and resolve RADIUS problems.
- If the switch gets no response in a specified time period after sending a stop-accounting request to a RADIUS server, it will buffer the request and transmit the buffered one until the maximum number of transmission attempts (set by the **retry stop-accounting** command) is reached.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Examples

Display the buffered stop-accounting requests generated from 0:0:0 08/31/2002 to 23:59:59 08/31/2002.

```
<Sysname>  display  stop-accounting-buffer  time-range  00:00:00-08/31/2002
23:59:59-08/31/2002
Total find    0 record
```

key

Syntax

key { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View

RADIUS scheme view

Parameters

accounting: Sets a shared key for RADIUS accounting messages.

authentication: Sets a shared key for RADIUS authentication/authorization messages.

string: Shared key to be set, a string of up to 16 characters.

Description

Use the **key** command to set a shared key for RADIUS authentication/authorization messages or accounting messages.

Use the **undo key** command to restore the corresponding default shared key setting.

By default, no shared key exists.

Note that:

- Both RADIUS client and server adopt MD5 algorithm to encrypt RADIUS messages before exchanging the messages with each other.
- The two parties verify the validity of the RADIUS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have same shared key.
- The authentication/authorization shared key and the accounting shared key you set on the switch must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

Related commands: **primary accounting**, **primary authentication**, **radius scheme**.

Examples

Set "hello" as the shared key for RADIUS authentication/authorization messages in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] key authentication hello
```

Set "ok" as the shared key for RADIUS accounting messages in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] key accounting ok
```

local-server

Syntax

local-server enable

undo local-server

View

System view

Parameters

None

Description

Use the **local-server enable** command to enable the UDP ports for local RADIUS services.

Use the **undo local-server** command to disable the UDP ports for local RADIUS services.

By default, the UDP ports for local RADIUS services are enabled.

In addition to functioning as a RADIUS client to provide remote RADIUS authentication, authorization, and accounting services, the switch can act as a local RADIUS server to provide simple RADIUS server functions locally. For the switch to act as a local server, you need to use this command to enable the service ports. The UDP port for local RADIUS authentication/authorization service is 1645, and that for local RADIUS accounting service is 1646.

Related commands: **radius scheme**, **state**, **local-server nas-ip**.

Examples

Enable UDP ports for local RADIUS services.

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

local-server nas-ip

Syntax

local-server nas-ip *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

View

System view

Parameters

nas-ip *ip-address*: Specifies the IP address of a network access server (NAS) that can use the local RADIUS services. Here, *ip-address* is in dotted decimal notation.

key *password*: Sets the shared key between the local RADIUS server and the NAS. Here, *password* is a string of up to 16 characters.

Description

Use the **local-server nas-ip** command to set the related parameters of the local RADIUS server.

Use the **undo local-server nas-ip** command to cancel a specified NAS setting for the local RADIUS server.

By default, the local RADIUS server is enabled and it allows the access of NAS 127.0.0.1. That is, the local device serves as both a RADIUS server and a network access server, and all authentications are performed locally. The default share key is null.

Note that:

- The message encryption key set by the **local-server nas-ip** *ip-address* **key** *password* command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this switch as its authentication server.
- The switch supports the IP addresses and shared keys of at most 16 network access servers (including the local device); that is, when the switch serves as a RADIUS server, it can provide authentication service to at most 16 NASs simultaneously.

- When serving as a local RADIUS server, the switch does not support EAP authentication.

Related commands: **radius scheme**, **state**, **local-server enable**.

Examples

Allow the local RADIUS server to provide services to NAS 10.110.1.2 with shared key aabbcc.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-server nas-ip 10.110.1.2 key aabbcc
```

nas-ip

Syntax

nas-ip *ip-address*

undo nas-ip

View

RADIUS scheme view

Parameters

ip-address: Source IP address for RADIUS messages, an IP address of this device. This address can neither be the all 0's address nor be a Class-D address.

Description

Use the **nas-ip** command to set the source IP address of outgoing RADIUS messages.

Use the **undo nas-ip** command to remove the source IP address setting.

By default, the IP address of the outbound interface is used as the source IP address of RADIUS messages.

Note

The **nas-ip** command in RADIUS scheme view has the same function as the **radius nas-ip** command in system view; and the configuration in RADIUS scheme view takes precedence over that in system view.

You can set the source IP address of outgoing RADIUS messages to avoid messages returned from RADIUS server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.

Related commands: **display radius scheme**, **radius nas-ip**.

Examples

Set source IP address 10.1.1.1 for outgoing RADIUS messages in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
```

```
New Radius scheme
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

primary accounting

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

RADIUS scheme view

Parameters

ip-address: IP address of the primary accounting server to be used, in dotted decimal notation.

port-number: UDP port number of the primary accounting server, ranging from 1 to 65535.

Description

Use the **primary accounting** command to set the IP address and port number of the primary RADIUS accounting server to be used by the current scheme.

Use the **undo primary accounting** command to restore the default IP address and port number of the primary RADIUS accounting server, which are 0.0.0.0 and 1813 respectively.

In the system default RADIUS scheme “system”, the default IP address of the primary accounting server is 127.0.0.1 and the default UDP port number is 1646. In a new RADIUS scheme, the default IP address of the primary accounting server is 0.0.0.0 and the default UDP port number is 1813.

Related commands: **key**, **radius scheme**, **state**.

Examples

Set the IP address and UDP port number of the primary accounting server for RADIUS scheme radius1 to 10.110.1.2 and 1813 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

primary authentication

Syntax

primary authentication *ip-address* [*port-number*]

undo primary authentication

View

RADIUS scheme view

Parameters

ip-address: IP address of the primary authentication/authorization server to be used, in dotted decimal notation.

port-number: UDP port number of the primary authentication/authorization server, ranging from 1 to 65535.

Description

Use the **primary authentication** command to set the IP address and port number of the primary RADIUS authentication/authorization server used by the current RADIUS scheme.

Use the **undo primary authentication** command to restore the default IP address and port number of the primary RADIUS authentication/authorization server, which are 0.0.0.0 and 1812 respectively.

In the system default RADIUS scheme “system”, the default IP address of the primary authentication/authorization server is 127.0.0.1 and the default UDP port number is 1645. In a new RADIUS scheme, the default IP address of the primary authentication/authorization server is 0.0.0.0 and the default UDP port number is 1812.

Note that:

- After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. For each kind of server, you can configure two servers in a RADIUS scheme: primary and secondary servers.
- In an actual network environment, you can make RADIUS server-related configuration as required. But you should configure at least one authentication/authorization server and one accounting server, and at the same time, you should keep the RADIUS server port settings on the switch consistent with those on the RADIUS servers.

Related commands: **key**, **radius scheme**, **state**.

Examples

Set the IP address and UDP port number of the primary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.1 and 1812 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

radius client

Syntax

radius client enable

undo radius client

View

System view

Parameters

None

Description

Use the **radius client enable** command to enable RADIUS authentication and accounting ports.

Use the **undo radius client** command to disable RADIUS authentication and accounting ports.

By default, RADIUS authentication and accounting ports are enabled.

If you want to use the switch as a RADIUS client, you need to ensure that the ports for RADIUS authentication and accounting are open. Otherwise, you can disable the ports to improve security of the switch.

Related commands: **radius scheme**.

Examples

Disable the RADIUS authentication and accounting ports.

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

radius nas-ip

Syntax

radius nas-ip *ip-address*

undo radius nas-ip

View

System view

Parameters

ip-address: Source IP address to be set, an IP address of this device. This address can neither be the all 0's address nor be a Class-D address.

Description

Use the **radius nas-ip** command to set the source IP address of outgoing RADIUS messages.

Use the **undo radius nas-ip** command to restore the default setting.

By default, no source IP address is set, and the IP address of corresponding outbound interface is used as the source IP address of RADIUS messages.

 **Note**

The **nas-ip** command in RADIUS scheme view has the same function as the **radius nas-ip** command in system view; and the configuration in RADIUS scheme view takes precedence over that in system view.

Note that:

- You can set the source IP address of outgoing RADIUS messages to avoid messages returned from RADIUS server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.
- You can set only one source IP address by using this command. When you re-execute this command again, the newly set source IP address will overwrite the old one.

Related commands: **nas-ip**.

Examples

Set source address 129.10.10.1 for outgoing RADIUS messages.

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

Parameters

radius-scheme-name: Name of the RADIUS scheme to be created, a string of up to 32 characters.

Description

Use the **radius scheme** command to create a RADIUS scheme and enter its view.

Use the **undo radius scheme** command to delete a specified RADIUS scheme.

By default, a RADIUS scheme named "system" has already been created in the system.

Note that:

- All the attributes of RADIUS scheme "system" take the default values, which you can see by using the **display radius scheme** command.
- The RADIUS protocol configuration is performed on a RADIUS scheme basis. For each RADIUS scheme, you should specify at least the IP addresses and UDP port numbers of the RADIUS authentication/authorization and accounting servers, and the parameters required for the RADIUS client to interact with the RADIUS servers. You should first create a RADIUS scheme and enter its view before performing RADIUS protocol configurations.
- A RADIUS scheme can be referenced by multiple ISP domains simultaneously.
- The **undo radius scheme** command cannot delete the default RADIUS scheme. In addition, you are not allowed to delete a RADIUS scheme which is being used by an online user.

Related commands: **key**, **retry realtime-accounting**, **scheme**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius scheme**, **display radius statistics**.

Examples

Create a RADIUS scheme named radius1 and enter its view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1]
```

radius trap

Syntax

radius trap { **authentication-server-down | accounting-server-down** }

undo radius trap { **authentication-server-down | accounting-server-down** }

View

System view

Parameters

authentication-server-down: Enables/disables the switch to send trap messages when a RADIUS authentication server turns down.

accounting-server-down: Enables/disables the switch to send trap messages when a RADIUS accounting server turns down.

Description

Use the **radius trap** command to enable the switch to send trap messages when a RADIUS server turns down.

Use the **undo radius trap** command to disable the switch from sending trap messages when a RADIUS authentication server or a RADIUS accounting server turns down.

By default, this function is disabled.

This configuration takes effect on all RADIUS scheme.

Note

The switch considers a RADIUS server as being down if it has tried the configured maximum number of times to send a message to the RADIUS server but does not receive any response.

Examples

Enable the switch to send trap messages when a RADIUS authentication server turns down.

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

reset radius statistics

Syntax

reset radius statistics

View

User view

Parameters

None

Description

Use the **reset radius statistics** command to clear RADIUS message statistics.

Related commands: **display radius scheme**.

Examples

Clear RADIUS message statistics.

```
<Sysname> reset radius statistics
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View

User view

Parameters

radius-scheme *radius-scheme-name*: Deletes the buffered stop-accounting requests of a specified RADIUS scheme. Here, *radius-scheme-name* is the name of a RADIUS scheme, which is a string of up to 32 characters that does not contain any of the following characters: /:*?<>.

session-id *session-id*: Deletes the buffered stop-accounting requests of a specified session. Here, *session-id* is a session ID, which is a string of up to 50 characters.

time-range *start-time stop-time*: Deletes the buffered stop-accounting requests generated within a specified time period. Here, *start-time* is the start time of the time period, *stop-time* is the end time of the time period, and both are in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Deletes the buffered stop-accounting requests of a specified user. Here, *user-name* is the name of a user, which is a string of up to 184 characters.

Description

Use the **reset stop-accounting-buffer** command to delete stop-accounting requests that are buffered on the switch due to getting no response.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Examples

Delete the stop-accounting requests buffered for user user0001@aabbcc.net.

```
<Sysname> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

Delete the stop-accounting requests buffered from 0:0:0 08/31/2002 to 23:59:59 08/31/2002.

```
<Sysname> reset stop-accounting-buffer time-range 00:00:00-08/31/2002 23:59:59-08/31/2002
```

retry

Syntax

retry *retry-times*

undo retry

View

RADIUS scheme view

Parameters

retry-times: Maximum number of transmission attempts of a RADIUS request, ranging from 1 to 20.

Description

Use the **retry** command to set the maximum number of transmission attempts of a RADIUS request.

Use the **undo retry** command to restore the default maximum number of transmission attempts.

By default, the maximum number of RADIUS request transmission attempts is 3.

Note that:

- The communication in RADIUS is unreliable because this protocol adopts UDP packets to carry its data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the server response timeout timer expires. If the switch gets no answer after it has tried the maximum number of times to transmit a RADIUS request, the switch considers that the request fails.
- Appropriately setting this maximum number of transmission attempts according to your network situation can improve the reacting speed of the system.

Related commands: **radius scheme**.

Examples

Set the maximum number of RADIUS request transmission attempts for RADIUS scheme radius1 to five.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax

retry realtime-accounting *retry-times*

undo retry realtime-accounting

View

RADIUS scheme view

Parameters

retry-times: Maximum allowed number of continuous real-time accounting failures, ranging from 1 to 255.

Description

Use the **retry realtime-accounting** command to set the maximum allowed number of continuous real-time accounting failures.

Use the **undo retry realtime-accounting** command to restore the default maximum number of continuous real-time accounting failures.

By default, the maximum number of continuous real-time accounting failures is five.

Note that:

- Generally, a RADIUS server uses the connection timeout timer to determine whether a user is currently online. If the RADIUS server receives no real-time accounting message for a specified period of time, it considers that the switch or the line is in trouble and stop accounting for the user. To make the switch cooperate with the RADIUS server in this feature, it is necessary to cut down the user connection on the switch to synchronize with the RADIUS server when the server terminates the accounting and connection of a user in case of unforeseen trouble. You can limit the number of continuous real-time accounting requests that fail due to getting no response, and then the switch will cut down user connection if the limit is reached.
- A real-time account request may be transmitted multiple times in an accounting attempt (the maximum number of transmission attempts is set by the **retry** command in RADIUS scheme view). If no response is received after the switch tries the maximum number of attempts to send the request, the switch considers the accounting fails. Suppose that the response timeout time of RADIUS server is three seconds (set by the **timer response-timeout** command), the maximum number of transmission attempts is 3 (set by the **retry** command), the real-time accounting interval is 12 minutes (set by the **timer realtime-accounting** command), the maximum allowed number of real-time accounting failures is 5 (set by the **retry realtime-accounting** command). In this case, the switch initiates an accounting request every 12 minutes; if the switch does not receive a response within 3 seconds after it sends out the accounting request, it resends the request; if the switch continuously sends the accounting request for three times but does not receive any response; it considers this real-time accounting a failure. Then, the switch reinitiates the accounting request every 12 minutes; if five continuous accounting failures occur, the switch cuts down the user connection.

Related commands: **radius scheme**, **timer realtime-accounting**.

Examples

Set the maximum allowed number of continuous real-time accounting failures for RADIUS scheme radius1 to 10.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
```

```
New Radius scheme
[Sysname-radius-radius1] retry realtime-accounting 10
```

retry stop-accounting

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

RADIUS scheme view

Parameters

retry-times: Maximum number of transmission attempts of a buffered stop-accounting request, ranging from 10 to 65,535.

Description

Use the **retry stop-accounting** command to set the maximum number of transmission attempts of a stop-accounting request buffered due to no response.

Use the **undo retry stop-accounting** command to restore the default maximum number of transmission attempts of a buffered stop-accounting request.

By default, the maximum number of stop-accounting request transmission attempts is 500.

Stop-accounting requests are critical to billing and will eventually affect the charges of users; they are important to both users and ISPs. Therefore, the switch should do its best to transmit them to RADIUS accounting servers. When getting no response to such a request, the switch should first buffer the request on itself, and then retransmit the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples

In RADIUS scheme radius1, specify that the switch can transmit a buffered stop-accounting request at most 1000 times

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] retry stop-accounting 1000
```

secondary accounting

Syntax

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

View

RADIUS scheme view

Parameters

ip-address: IP address of the secondary accounting server to be used, in dotted decimal notation.

port-number: UDP port number of the secondary accounting server, ranging from 1 to 65535.

Description

Use the **secondary accounting** command to set the IP address and port number of the secondary RADIUS accounting server to be used by the current scheme.

Use the **undo secondary accounting** command to restore the default IP address and port number of the secondary RADIUS accounting server, which are 0.0.0.0 and 1813 respectively.

Related commands: **key**, **radius scheme**, **state**.

Examples

Set the IP address and UDP port number of the secondary accounting server for RADIUS scheme radius1 to 10.110.1.1 and 1813 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

secondary authentication

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

RADIUS scheme view

Parameters

ip-address: IP address of the secondary authentication/authorization server to be used, in dotted decimal notation.

port-number: UDP port number of the secondary authentication/authorization server, ranging from 1 to 65535.

Description

Use the **secondary authentication** command to set the IP address and port number of the secondary RADIUS authentication/authorization server to be used by the current scheme.

Use the **undo secondary authentication** command to restore the default IP address and port number of the secondary RADIUS authentication/authorization server, which is 0.0.0.0 and 1812 respectively.

Related commands: **key**, **radius scheme**, **state**.

Examples

Set the IP address and UDP port number of the secondary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.2 and 1812 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

server-type

Syntax

server-type { **extended** | **standard** }

undo server-type

View

RADIUS scheme view

Parameters

extended: Specifies to support H3C's RADIUS server (which is generally a CAMS), that is, use the procedure and message format of private RADIUS protocol to interact with an H3C's RADIUS server.

standard: Specifies to support standard RADIUS server, that is, use the procedure and message format of a standard RADIUS protocol (RFC 2865/2866 or above) to interact with a standard RADIUS server.

Description

Use the **server-type** command to configure the switch to support a specified type of RADIUS server.

Use the **undo server-type** command to restore the default setting.

By default, the switch supports RADIUS servers of the standard type, and the RADIUS server type in the default scheme named **system** is extended.

Related commands: **radius scheme**.

Examples

Configure the switch to support H3C's RADIUS server in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] server-type extended
```

state

Syntax

state { **primary** | **secondary** } { **accounting** | **authentication** } { **block** | **active** }

View

RADIUS scheme view

Parameters

primary: Specifies that the server to be set is a primary RADIUS server.

secondary: Specifies that the server to be set is a secondary RADIUS server.

accounting: Specifies that the server to be set is a RADIUS accounting server.

authentication: Specifies that the server to be set is a RADIUS authentication/authorization server.

block: Sets the status of the specified RADIUS server to **block** (that is, the down state).

active: Sets the status of the specified RADIUS server to **active** (that is, the normal working state).

Description

Use the **state** command to set the status of a RADIUS server.

By default, all RADIUS servers in any customized RADIUS scheme are in the **block** state; the primary RADIUS servers in the default RADIUS scheme "system" are in the **active** state, and the secondary RADIUS servers in "system" are in the **block** state.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme, note that:

- When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.
- After the primary server remains in the block state for a set time (set by the **timer quiet** command), the switch will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to active while keeping the status of the secondary server unchanged.
- When both primary and secondary servers are in the active or block state, the switch sends messages only to the primary server.

Related commands: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

Examples

Set the status of the secondary authentication server in RADIUS scheme radius1 to **active**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] state secondary authentication active
```

stop-accounting-buffer enable

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

RADIUS scheme view

Parameters

None

Description

Use the **stop-accounting-buffer enable** command to enable the switch to buffer the stop-accounting requests that get no response.

Use the **undo stop-accounting-buffer enable** command to disable the switch from buffering the stop-accounting requests that get no response.

By default, the switch is enabled to buffer the stop-accounting requests that get no response.

Stop-accounting requests are critical to billing and will eventually affect the charges; they are important to both users and ISPs. Therefore, the switch should do its best to transmit them to RADIUS accounting servers. When getting no response to such a request, the switch should first buffer the request on itself, and then retransmit the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples

In RADIUS scheme radius1, enable the switch to buffer the stop-accounting requests that get no response from the servers.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer

Syntax

timer *seconds*

undo timer

View

RADIUS scheme view

Parameters

seconds: Response timeout time of RADIUS servers, ranging from 1 to 10 seconds.

Description

Use the **timer** command to set the response timeout time of RADIUS servers (that is, the timeout time of the response timeout timer of RADIUS servers).

Use the **undo timer** command to restore the default response timeout timer of RADIUS servers.

By default, the response timeout time of RADIUS servers is 3 seconds.

Note that:

- After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the switch waits for a response from the server. The maximum time that the switch can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the switch system is called the response timeout timer of RADIUS servers. You can use the **timer** command to set the timeout time of this timer, and if the switch gets no answer before the response timeout timer expires, it needs to retransmit the request to ensure that the user can obtain RADIUS service.
- Appropriately setting the timeout time of this timer according to your network situation can improve the performance of your system.
- The **timer** command has the same function with the **timer response-timeout** command.

Related commands: **radius scheme**, **retry**.

Examples

Set the timeout time of the response timeout timer for RADIUS scheme radius1 to 5 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] timer 5
```

timer quiet

Syntax

timer quiet *minutes*

undo timer quiet

View

RADIUS scheme view

Parameters

minutes: Wait time before primary server state restoration, ranging from 1 to 255 minutes.

Description

Use the **timer quiet** command to set the time that the switch waits before it tries to re-communicate with the primary server and restore the status of the primary server to active.

Use the **undo timer quiet** command to restore the default wait time.

By default, the switch waits five minutes.

Related commands: **display radius scheme**.

Examples

Configure the switch to wait 10 minutes before it tries to restore the status of the primary server to active.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] timer quiet 10
```

timer realtime-accounting

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

RADIUS scheme view

Parameters

minutes: Real-time accounting interval, in minutes. It ranges from 3 to 60 and must be a multiple of 3.

Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default real-time accounting interval.

By default, this interval is 12 minutes.

Note that:

- To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users' accounting information to the RADIUS server at the set interval.
- The setting of the real-time accounting interval depends, to some degree, on the performance of the switch and the RADIUS server. The higher the performance of the switch and the RADIUS server is, the shorter the interval can be. It is recommended to set the interval as long as possible when the number of users is relatively great (≥1000). Table 1-6 lists the recommended intervals for different numbers of users.

Table 1-6 Numbers of users and recommended intervals

Number of users	Real-time accounting interval
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

Related commands: **retry realtime-accounting**, **radius scheme**.

Examples

Set the real-time accounting interval of RADIUS scheme radius1 to 51 minutes.

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

```
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

RADIUS scheme view

Parameters

seconds: Response timeout time of RADIUS servers, ranging from 1 to 10 seconds.

Description

Use the **timer response-timeout** command to set the response timeout time of RADIUS servers.

Use the **undo timer response-timeout** command to restore the default response timeout time of RADIUS servers.

By default, the response timeout time of RADIUS servers is 3 seconds.

Note that:

- After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the switch waits for a response from the server. The maximum time that the switch can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the switch system is called the response timeout timer of RADIUS servers. You can use the **timer response-timeout** command to set the timeout time of this timer, and if the switch gets no answer before the response timeout timer expires, it needs to retransmit the request to ensure that the user can obtain RADIUS service.
- Appropriately setting the timeout time of this timer according to your network situation can improve the performance of your system.
- This command has the same function with the **timer** command.

Related commands: **radius scheme**, **retry**.

Examples

Set the response timeout time in RADIUS scheme radius1 to five seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format

Syntax

user-name-format { **with-domain** | **without-domain** }

View

RADIUS scheme view

Parameters

with-domain: Specifies to include ISP domain names in the usernames to be sent to RADIUS server.

without-domain: Specifies to exclude ISP domain names from the usernames to be sent to RADIUS server.

Description

Use the **user-name-format** command to set the format of the usernames to be sent to RADIUS server

By default, except for the default RADIUS scheme "system", the usernames sent to RADIUS servers in any RADIUS scheme carry ISP domain names.

Note that:

- Generally, an access user is named in the *userid@isp-name* format. Here, *isp-name* behind the @ character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old RADIUS servers cannot accept the usernames that carry ISP domain names. In this case, it is necessary to remove domain names from usernames before sending usernames to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the usernames to be sent to the RADIUS server.
- For a RADIUS scheme, if you have specified to exclude ISP domain names from usernames, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).
- For an 802.1x user, if you have specified to use EAP authentication, the switch will encapsulate and send the contents from the client directly to the server. In this case, the configuration of the **user-name-format** command is not effective.

Related commands: **radius scheme**.

Examples

Specify to exclude ISP domain names from the usernames to be sent to RADIUS server in RADIUS scheme radius1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] user-name-format without-domain
```

HWTACACS Configuration Commands

data-flow-format

Syntax

data-flow-format data { **byte | giga-byte | kilo-byte | mega-byte** }

data-flow-format packet { **giga-packet | kilo-packet | mega-packet | one-packet** }

undo data-flow-format { data | packet }

View

HWTACACS scheme view

Parameters

data: Sets the data unit of outgoing HWTACACS data flows, which can be byte, giga-byte, kilo-byte, or mega-byte.

packet: Sets the packet unit of outgoing HWTACACS data flows, which can be one-packet, giga-packet, kilo-packet, or mega-packet.

Description

Use the **data-flow-format** command to set the units of data flows to TACACS servers.

Use the **undo data-flow-format** command to restore the default units.

By default, the data unit and packet unit for outgoing HWTACACS flows are byte and one-packet respectively.

Note that the specified unit of data flows sent to the TACACS server must be consistent with the traffic statistics unit of the TACACS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display hwtacacs**.

Examples

Specify to measure data and packets in data flows to TACACS servers in kilo-bytes and kilo-packets respectively in HWTACACS scheme hwt1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname- hwtacacs-hwt1] data-flow-format data kilo-byte
[Sysname- hwtacacs-hwt1] data-flow-format packet kilo-packet
```

display hwtacacs

Syntax

display hwtacacs [*hwtacacs-scheme-name* [**statistics**]]

View

Any view

Parameters

hwtacacs-scheme-name: HWTACACS scheme name, a string of 1 to 32 characters. This name is case-insensitive. If this argument is not specified, the system displays information about all HWTACACS schemes.

statistics: Displays statistics about one or all HWTACACS schemes.

Description

Use the **display hwtacacs** command to display configuration or statistics information of one specified or all HWTACACS schemes.

Related commands: **hwtacacs scheme**.

Examples

Display configuration information of HWTACACS scheme ht1.

```
<Sysname> display hwtacacs ht1
-------------------------------------------------------------------     HWTACACS-server
template name   : ht1
  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
  Source-IP-address               : 0.0.0.0
  key authentication              : 790131
  key authorization               : 790131
  key accounting                  : 790131
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Realtime-accouting-Interval(min): 12
  Stop-acct-PKT resending times   : 100
  Domain-included                 : No
  Traffic-unit                    : B
  Packet traffic-unit             : one-packet
```

display stop-accounting-buffer

Syntax

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

View

Any view

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Displays the buffered stop-accounting requests of a specified HWTACACS scheme. Here, *hwtacacs-scheme-name* is a string of up to 32 characters.

Description

Use the **display stop-accounting-buffer** command to display stop-accounting requests buffered in the switch.

Related commands: reset stop-accounting-buffer, stop-accounting-buffer enable, retry stop-accounting.

Examples

Display stop-accounting requests buffered for HWTACACS scheme hwt1.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
```

hwtacacs nas-ip

Syntax

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip

View

System view

Parameters

ip-address: Source IP address to be set, an IP address of this device. This address can neither be the all 0's address nor be a Class D address.

Description

Use the **hwtacacs nas-ip** command to set the source address of outgoing HWTACACS messages.

Use the **undo hwtacacs nas-ip** command to restore the default setting.

By default, no source address is specified, and the IP address of corresponding outbound interface is used as the source address.

Note that:

- You can specify the source address of outgoing HWTACACS messages to avoid messages returned from server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.
- You can specify only one source IP address by using this command. When you re-execute this command again, the newly set source IP address will overwrite the old one.

Related commands: **nas-ip**.

Examples

Configure the switch to use source address 129.10.10.1 for outgoing HWTACACS messages.

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

Parameters

hwtacacs-scheme-name: HWTACACS scheme name, a string of 1 to 32 characters.

Description

Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter its view.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

Examples

Create an HWTACACS scheme named "hwt1" and enter the corresponding HWTACACS scheme view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

key

Syntax

key { **accounting** | **authentication** | **authorization** } *string*

undo key { accounting | authentication | authorization }

View

HWTACACS scheme view

Parameters

accounting: Sets a shared key for HWTACACS accounting messages.

authentication: Sets a shared key for HWTACACS authentication messages.

authorization: Sets a shared key for HWTACACS authorization messages.

string: Shared key to be set, a string of up to 16 characters.

Description

Use the **key** command to configure a shared key for HWTACACS authentication, authorization or accounting messages.

Use the **undo key** command to delete such a configuration.

By default, no key is set for HWTACACS messages.

Related commands: **display hwtacacs**.

Examples

Use hello as the shared key for HWTACACS accounting messages in HWTACACS scheme hwt1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

nas-ip

Syntax

nas-ip ip-address

undo nas-ip

View

HWTACACS scheme view

Parameters

ip-address: Source IP address to be set, an IP address of this device. This address can neither be the all 0's address nor be a Class D address.

Description

Use the **nas-ip** command to set the source address of outgoing HWTACACS messages.

Use the **undo nas-ip** command to restore the default setting.

Note that:

- You can set the source address of HWTACACS messages to avoid messages returned from server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.
- You can set only one source IP address by using this command. When you re-execute this command again, the newly set source IP address will overwrite the old one.

Related commands: **display hwtacacs**.

Examples

Set source IP address 10.1.1.1 for outgoing HWTACACS messages in HWTACACS scheme hwt1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

primary accounting

Syntax

primary accounting *ip-address* [*port*]

undo primary accounting

View

HWTACACS scheme view

Parameters

ip-address: IP address of the primary accounting server to be used, a valid unicast address in dotted decimal notation.

port: Port number of the primary accounting server, ranging from 1 to 65535.

Description

Use the **primary accounting** command to set the IP address and port number of the primary HWTACACS accounting server to be used by the current scheme.

Use the **undo primary accounting** command to restore the default IP address and port number of the primary HWTACACS accounting server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary accounting servers. If you do this, your setting will fail.
- If you re-execute the command, the new setting will overwrite the old one.
- You can remove an accounting server setting only when there is no active TCP connection that is sending accounting messages to the server.

Examples

Set the IP address and UDP port number of the primary accounting server for HWTACACS scheme test1 to 10.163.155.12 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication

Syntax

primary authentication *ip-address* [*port*]

undo primary authentication

View

HWTACACS scheme view

Parameters

ip-address: IP address of the primary authentication server to be used, a valid unicast address in dotted decimal notation.

port: Port number of the primary authentication server, ranging from 1 to 65535.

Description

Use the **primary authentication** command to set the IP address and port number of the primary HWTACACS authentication server to be used by the current scheme.

Use the **undo primary authentication** command to restore the default IP address and port number of the primary HWTACACS authentication server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary authentication servers. If you do this, your setting will fail.
- If you re-execute the command, the new setting will overwrite the old one.
- You can remove an authentication server setting only when there is no active TCP connection that is sending authentication messages to the server.

Related commands: **display hwtacacs**.

Examples

Set the IP address and UDP port number of the primary authentication server for HWTACACS scheme hwt1 to 10.163.155.13 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax

primary authorization *ip-address* [*port*]

undo primary authorization

View

HWTACACS scheme view

Parameters

ip-address: IP address of the primary authorization server to be used, a valid unicast address in dotted decimal notation.

port: Port number of the primary authorization server, ranging from 1 to 65535.

Description

Use the **primary authorization** command to set the IP address and port number of the primary HWTACACS authorization server to be used by the current scheme.

Use the **undo primary authorization** command to restore the default IP address and port number of the primary authorization server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary authorization servers. If you do this, your setting will fail.
- If you re-execute the command, the new setting will overwrite the old one.
- You can remove an authorization server setting only when there is no active TCP connection that is sending authorization messages to the server.

Related commands: **display hwtacacs**.

Examples

Set the IP address and UDP port number of the primary authorization server for HWTACACS scheme hwt1 to 10.163.155.13 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax

reset hwtacacs statistics { accounting | authentication | authorization | all }

View

User view

Parameters

accounting: Clears HWTACACS accounting statistics.

authentication: Clears HWTACACS authentication statistics.

authorization: Clears HWTACACS authorization statistics.

all: Clears all HWTACACS statistics.

Description

Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

Examples

Clear all HWTACACS protocol statistics.

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

View

User view

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Deletes the buffered stop-accounting requests of a specified HWTACACS scheme. Here, *hwtacacs-scheme-name* is the name of a HWTACACS scheme, which is a string of up to 32 characters.

Description

Use the **reset stop-accounting-buffer** command to clear stop-accounting requests that are buffered on the switch due to getting no response.

Related commands: stop-accounting-buffer enable, retry stop-accounting, display stop-accounting-buffer.

Examples

Delete the stop-accounting requests buffered for HWTACACS scheme hwt1.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

HWTACACS scheme view

Parameters

retry-times: Maximum number of transmission attempts of a stop-accounting request, ranging from 1 to 300.

Description

Use the **retry stop-accounting** command to enable the stop-accounting request retransmission function and set the maximum number of attempts to transmit a stop-accounting request.

Use the **undo retry stop-accounting** command to restore the default setting.

By default, this function is enabled and the maximum number of transmission attempts is 100.

Related commands: reset stop-accounting-buffer, hwtacacs scheme, display stop-accounting-buffer.

Examples

Enable the stop-accounting request retransmission function and set the maximum number of transmission attempts of a request to 50.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting

Syntax

secondary accounting *ip-address* [*port*]

undo secondary accounting

View

HWTACACS scheme view

Parameters

ip-address: IP address of the secondary accounting server to be used, a valid unicast address in dotted decimal notation.

port: Port number of the secondary accounting server, ranging from 1 to 65535.

Description

Use the **secondary accounting** command to set the IP address and port number of the secondary HWTACACS accounting server to be used by the current scheme.

Use the **undo secondary accounting** command to restore the default IP address and port number of the secondary HWTACACS accounting server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary accounting servers. If you do this, your setting will fail.
- If you re-execute the command, the new setting will overwrite the old one.
- You can remove an accounting server setting only when there is no active TCP connection that is sending accounting messages to the server.

Examples

Set the IP address and UDP port number of the secondary accounting server for HWTACACS scheme hwt1 to 10.163.155.12 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication

Syntax

secondary authentication *ip-address* [*port*]

undo secondary authentication

View

HWTACACS scheme view

Parameters

ip-address: IP address of the secondary authentication server to be used, a valid unicast address in dotted decimal notation.

port: Port number of the secondary authentication server, ranging from 1 to 65535.

Description

Use the **secondary authentication** command to set the IP address and port number of the secondary HWTACACS authentication server to be used by the current scheme.

Use the **undo secondary authentication** command to restore the default IP address and port number of the secondary HWTACACS authentication server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary authentication servers. If you do this, your setting will fail.
- If you re-execute the command, the new setting overwrites the old one.
- You can remove an authentication server setting only when there is no active TCP connection that is sending authentication messages to the server.

Related commands: **display hwtacacs**.

Examples

Set the IP address and UDP port number of the secondary authentication server for HWTACACS scheme hwt1 to 10.163.155.13 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax

secondary authorization *ip-address* [*port*]

undo secondary authorization

View

HWTACACS scheme view

Parameters

ip-address: IP address of the secondary authorization server, a valid unicast address in dotted decimal notation.

port: Port number of the secondary authorization server, ranging from 1 to 65535.

Description

Use the **secondary authorization** command to set the IP address and port number of the secondary HWTACACS authorization server to be used by the current scheme.

Use the .**undo secondary authorization** command to restore the default IP address and port number of the secondary HWTACACS authorization server, which are 0.0.0.0 and 49 respectively.

Note that:

- You are not allowed to set the same IP address for both primary and secondary authorization servers.
- If you re-execute the command, the new setting will overwrite the old one.
- You can remove an authorization server setting only when there is no active TCP connection that is sending authorization messages to the server.

Related commands: **display hwtacacs**.

Examples

Set the IP address and UDP port number of the secondary authorization server for HWTACACS scheme hwt1 to 10.163.155.13 and 49 respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

timer quiet

Syntax

timer quiet *minutes*

undo timer quiet

View

HWTACACS scheme view

Parameters

minutes: Wait time before primary server state restoration, ranging from 1 to 255 minutes.

Description

Use the **timer quiet** command to set the time that the switch waits before it tries to re-communicate with the primary server and restore the status of the primary server to active.

Use the **undo timer quiet** command to restore the default wait time.

By default, the switch waits five minutes.

Related commands: **display hwtacacs**.

Examples

Configure the switch to wait 10 minutes before it tries to restore the status of the primary server to active.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet  10
```

timer realtime-accounting

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

HWTACACS scheme view

Parameters

minutes: Real-time accounting interval, in minutes. It ranges from 3 to 60 and must be a multiple of 3.

Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default real-time accounting interval.

By default, the real-time accounting interval is 12 minutes.

Note that:

- To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users' accounting information to TACACS accounting server at the set interval.
- The setting of the real-time accounting interval depends, to some degree, on the performance of the switch and the TACACS server. The higher the performance of the switch and the TACACS server is, the shorter the interval can be. It is recommended to set the interval as long as possible when the number of users is relatively great (≥1000). The following table lists the recommended intervals for different numbers of users.

Table 1-7 Numbers of users and recommended intervals

Number of users	Real-time accounting interval
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

Examples

Set the real-time accounting interval in HWTACACS scheme hwt1 to 51 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

HWTACACS scheme view

Parameters

seconds: Response timeout time of TACACS servers, ranging from 1 to 300 seconds.

Description

Use the **timer response-timeout** command to set the response timeout time of TACACS servers.

Use the **undo timer response-timeout** command to restore the default response timeout time of TACACS servers.

By default, the response timeout time of TACACS servers is five seconds.

As HWTACACS is based on TCP, both server response timeout and TCP timeout may cause disconnection from TACACS server.

Related commands: **display hwtacacs**.

Examples

Set the response timeout time of TACACS servers to 30 seconds for HWTACACS scheme hwt1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format

Syntax

user-name-format { with-domain | without-domain }

View

HWTACACS scheme view

Parameters

with-domain: Specifies to include ISP domain names in the usernames to be sent to TACACS server.

without-domain: Specifies to exclude ISP domain names from the usernames to be sent to TACACS server.

Description

Use the **user-name-format** command to set the format of the usernames to be sent to TACACS server.

By default, the usernames sent to TACACS server in a HWTACACS scheme carry ISP domain names.

Note that:

- Generally, an access user is named in the *userid@isp-name* format. Here, *isp-name* behind the @ character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old TACACS servers cannot accept the usernames that carry ISP domain names. In this case, it is necessary to remove domain names from usernames before sending usernames to TACACS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the usernames to be sent to TACACS server.
- For a HWTACACS scheme, if you have specified to exclude ISP domain names from usernames, you should not use this scheme in more than one ISP domain. Otherwise, such errors may occur: the TACACS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).

Related commands: **hwtacacs scheme**.

Examples

Specify to exclude ISP domain names from the usernames to be sent to TACACS server in HWTACACS scheme hwt1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

2 EAD Configuration Commands

EAD Configuration Commands

security-policy-server

Syntax

security-policy-server *ip-address*

undo security-policy-server { *ip-address* | all }

View

RADIUS scheme view

Parameters

ip-address: IP address of a security policy server.

all: IP addresses of all security policy servers.

Description

Use the **security-policy-server** command to set the IP address of a security policy server.

Use the **undo security-policy-server** command to remove one specified or all security policy server address settings.

You can configure up to eight security policy server addresses in each RADIUS scheme. The switch only responds to those session control messages that come from authentication server or security policy server.

Examples

Set a security policy server address 192.168.0.1 on the switch.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme extended
[Sysname-radius-extended] security-policy-server 192.168.0.1
[Sysname-radius-extended] display current-configuration
…
radius scheme extended
primary authentication 1.1.11.29 1812
secondary authentication 127.0.0.1 1645
security-policy-server 192.168.0.1
user-name-format without-domain
…
```

Table of Contents

1 MAC Address Authentication Configuration Commands

MAC Address Authentication Basic Function Configuration Commands

display mac-authentication

Syntax

display mac-authentication [**interface** *interface-list*]

View

Any view

Parameters

interface *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **display mac-authentication** command to display information about MAC address authentication.

Examples

Display the global information about MAC address authentication.

```
<Sysname> display mac-authentication
Mac address authentication is Enabled.
 Authentication mode is UsernameAsMacAddress
 Usernameformat:with-hyphen lowercase
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60 second(s).
         Server response timeout value  is 100s
         Guest VLAN re-authenticate period is 30s
         Max allowed user number is 1024
         Current user number amounts to  1
         Current domain: not configured, use default domain
Silent Mac User info:
          MAC ADDR            From Port               Port Index
          --- On unit 1, 1 silent mac address(es) found. ---
```

```
          0016-e0be-e201       GigabitEthernet1/0/2              1(vlan:1)
          --- 1 silent mac address(es) found. ---
GigabitEthernet1/0/1 is link-up
  MAC address authentication  is Enabled
  max-auth-num is 256
  Guest VLAN is 2
  Authenticate success: 1, failed: 0
  Current online user number is 1
    MAC ADDR         Authenticate state           AuthIndex
    000d-88f8-4e71   MAC_AUTHENTICATOR_SUCCESS     0
```

……(The following is omitted)

Table 1-1 Description on the fields of the **display mac-authentication** command

Field	Description
Mac address authentication is Enabled	MAC address authentication is enabled.
Authentication mode	Username type used in the MAC address authentication: • UsernameFixed: Uses the fixed username for authentication. • UsernameAsMacAddress: Uses the MAC address of a user as the username for authentication. The default is the MAC address (UsernameAsMacAddress).
Fixed password	Meaning of this field varies by the username type for MAC address authentication: • If the username type is MAC address, this field indicates whether to use a fixed password for authentication. By default, this field is not configured, which means using the MAC address of a user as the password for authentication. • If the username type is fixed username, this field indicates whether a fixed password is configured. By default, this field is not configured, which means the password is null.
Fixed password	Password used in the fixed mode, which is not configured by default.
Offline detect period	Offline detect timer, which sets the time interval to check whether a user goes offline and defaults to 300 seconds.
Quiet period	Quiet timer sets the quiet period. A switch goes through a quiet period if a user fails to pass the MAC address authentication. The default value is 60 seconds.
Server response timeout value	Server timeout timer, which sets the timeout time for the connection between a switch and the RADIUS server. By default, it is 100 seconds.
Guest VLAN re-authenticate period	Re-authenticate timer, which sets the time interval to reauthenticate the users in the Guest VLAN and defaults to 30 seconds.

Field	Description
Max allowed user number	The maximum number of users supported by the switch. It is 1,024 by default.
Current user number amounts to	The current number of users
Current domain	The current domain. It is not configured by default.
Silent Mac User info	The information about the silent user. When the user fails to pass MAC address authentication because of inputting error user name and password, the switch sets the user to be in quiet state. During quiet period, the switch does not process the authentication request of this user.
GigabitEthernet1/0/1 is link-up	The link connected to GigabitEthernet1/0/1 port is up.
MAC address authentication is Enabled	MAC address authentication is enabled for GigabitEthernet1/0/1 port.
max-auth-num	Maximum number of MAC address authentication users that the port can accommodate
Guest VLAN	Guest VLAN of the port
Authenticate success: 1, failed: 0	Statistics of the MAC address authentications performed on the port, including the numbers of successful and failed authentication operations.
Current online user number	The number of the users current access the network through the port
MAC ADDR	Peer MAC address
Authenticate state	The state of the users accessing the network through the port, which can be: • MAC_AUTHENTICATOR_CONNECTING: Connecting • MAC_AUTHENTICATOR_SUCCESS: Authentication passed • MAC_AUTHENTICATOR_FAILURE: Fail to pass authentication • MAC_AUTHENTICATOR_LOGOFF: Offline
AuthIndex	Index of the current MAC address with regard to the authentication port

mac-authentication

Syntax

mac-authentication

undo mac-authentication

View

System view, Ethernet port view

Parameters

None

Description

Use the **mac-authentication** command to enable MAC address authentication globally or on the current port.

Use the **undo mac-authentication** command to disable MAC address authentication globally or on the current port.

By default, MAC address authentication is disabled both globally and on a port.

When being executed in system view, the **mac-authentication** command enables MAC address authentication globally.

When being executed in Ethernet port view, the **mac-authentication** command enables MAC address authentication on the current port.

To make the MAC address authentication take effect, you must enable MAC address authentication globally and on the relevant ports.

Note

You can configure MAC address authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC address authentication is enabled globally.

Examples

Enable MAC address authentication globally.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-authentication
  MAC-Authentication is enabled globally.
```

Enable MAC address authentication on port GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

mac-authentication interface

Syntax

mac-authentication interface *interface-list*

undo mac-authentication interface *interface-list*

View

System view

Parameters

interface-list: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **mac-authentication interface** command to enable the MAC address authentication for on the specified port(s).

Use the **undo mac-authentication interface** command to disable the MAC address authentication for the specified port(s).

By default, MAC address authentication is disabled on a port.

Note

- This command is essential for MAC address authentication to work on a port or on particular ports after MAC address authentication is globally enabled.
- You cannot configure the maximum number of dynamic MAC address entries for a port (through the **mac-address max-mac-count** command) with MAC address authentication enabled. Likewise, you cannot enable the MAC address authentication feature on a port with a limit of dynamic MAC addresses configured.
- If you have enabled MAC address authentication on a port, you cannot add the port to an aggregation group. If a port is already added to an aggregation group, you cannot enable MAC address authentication on the port.

Examples

Enable MAC address authentication for GigabitEthernet1/0/1 port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-authentication interface GigabitEthernet 1/0/1
```

mac-authentication authmode usernameasmacaddress

Syntax

mac-authentication authmode usernameasmacaddress [**usernameformat** { **with-hyphen** | **without-hyphen** }] { **lowercase** | **uppercase** } | **fixedpassword** *password*]

undo mac-authentication authmode usernameasmacaddress [**usernameformat** | **fixedpassword**]

View

System view

Parameters

usernameformat: Specifies the input format of the username and password.

with-hyphen: Uses hyphened MAC addresses as usernames and passwords, for example, 00-05-e0-1c-02-e3.

without-hyphen: Uses MAC addresses without hyphens as usernames and passwords, for example, 0005e01c02e3.

lowercase: Uses lowercase MAC addresses as usernames and passwords.

uppercase: Uses uppercase MAC addresses as usernames and passwords.

fixedpassword *password*: Specifies the password for MAC address authentication as the specified fixed password instead of user MAC addresses. *password i*s a string of 1 to 63 characters.

Description

Use the **mac-authentication authmode usernameasmacaddress** command to set the username type for MAC address authentication to MAC address and specify the username format.

Use the **undo mac-authentication authmode** command to restore the default user name mode.

By default, the user name and password in MAC address mode are used for MAC address authentication.

Examples

Use the user name in MAC address mode for MAC address authentication, requiring hyphened lowercase MAC addresses as the usernames and passwords.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen
lowercase
```

mac-authentication authmode usernamefixed

Syntax

mac-authentication authmode usernamefixed

undo mac-authentication authmode

View

System view

Parameters

None

Description

Use the **mac-authentication authmode usernamefixed** command to set the user name in fixed mode for MAC address authentication.

Use the **undo mac-authentication authmode** command to restore the default user name mode for MAC address authentication.

By default, the MAC address mode is used.

Examples

Use the user name in fixed mode for MAC address authentication.

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

mac-authentication authpassword

Syntax

mac-authentication authpassword *password*

undo mac-authentication authpassword

View

System view

Parameters

password: Password to be set, a string comprising 1 to 63 characters.

Description

Use the **mac-authentication authpassword** command to set a password for MAC address authentication when the user name in fixed mode is used.

Use the **undo mac-authentication authpassword** command to cancel the configured password.

By default, no password is configured.

Examples

Set the password to **newmac**.

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

mac-authentication authusername

Syntax

mac-authentication authusername *username*

undo mac-authentication authusername

View

System view

Parameters

username: User name used in authentication, a string of 1 to 55 characters.

Description

Use the **mac-authentication authusername** command to set a user name in fixed mode.

Use the **undo mac-authentication authusername** command to restore the default user name.

By default, the user name in fixed mode is “mac”.

Examples

Set the user name to **vipuser** in fixed mode.

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

mac-authentication domain

Syntax

mac-authentication domain *isp-name*

undo mac-authentication domain

View

System view

Parameters

isp-name: ISP domain name, a string of 1 to 128 characters. Note that this argument cannot be null and cannot contain these characters: “/”, “:”, “*”, “?”, “<”, and “>”.

Description

Use the **mac-authentication domain** command to configure an ISP domain for MAC address authentication.

Use the **undo mac-authentication domain** command to restore the default ISP domain for MAC address authentication.

By default, no domain for MAC address authentication is configured.

Use the “default domain” as the ISP domain name.

Examples

Configure the domain for MAC address authentication to be **aabbcc**.

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

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

Parameters

offline-detect-value: Offline detect timer (in seconds) setting. This argument ranges from 1 to 65,535 and defaults to 300. The offline detect timer sets the time interval for a switch to test whether a user goes offline.

quiet-value: Quiet timer (in seconds) setting. This argument ranges from 1 to 3,600 and defaults to 60. After a user fails to pass the authentication performed by a switch, the switch quiets for a specific period (the quiet period) before it authenticates the user again.

server-timeout-value: Server timeout timer setting (in seconds). This argument ranges from 1 to 65,535 and defaults to 100. During authentication, the switch prohibits a user from accessing the network if the connection between the switch and the RADIUS server times out.

Description

Use the **mac-authentication timer** command to configure the timers used in MAC address authentication.

Use the **undo mac-authentication timer** command to restore a timer to its default setting.

Related commands: **display mac-authentication**.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-authentication timer server-timeout 150
```

reset mac-authentication

Syntax

reset mac-authentication statistics [**interface** *interface-list*]

View

User view

Parameters

interface-list: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **reset mac-authentication** command to clear the MAC address authentication statistics. With the **interface** keyword specified, the command clears the MAC address authentication statistics of the specified port. Without this keyword, the command clears the global MAC address authentication statistics.

Examples

Clear the MAC address authentication statistics for port GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface GigabitEthernet 1/0/1
```

MAC Address Authentication Enhanced Function Configuration Commands

mac-authentication guest-vlan

Syntax

mac-authentication guest-vlan *vlan-id*

undo mac-authentication guest-vlan

View

Ethernet port view

Parameters

vlan-id: ID of the guest VLAN configured for the current port. This argument is in the range of 1 to 4,094.

Description

Use the **mac-authentication guest-vlan** command to configure a guest VLAN for the current port. If the client connected to the port fails in the authentication, the port will be added to the guest VLAN, and thus the users accessing the port can access network resources in the guest VLAN.

Use the **undo mac-authentication guest-vlan** command to remove the guest VLAN configuration for the port.

No guest VLAN is configured for a port by default.

The system will re-authenticate users in the guest VLAN at the interval configured by the **mac-authentication timer guest-vlan-reauth** command. If the user of a port passes the authentication, the port will leave the guest VLAN and return to the initial VLAN configured for it.

Caution

- If more than one client are connected to a port, you cannot configure a Guest VLAN for this port.
- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.
- The **undo vlan** command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to the VLAN module in this manual for the description on the **undo vlan** command.
- Only one Guest VLAN can be configured for a port, and the VLAN configured as the Guest VLAN must be an existing VLAN. Otherwise, the Guest VLAN configuration does not take effect. If you want to change the Guest VLAN for a port, you must remove the current Guest VLAN and then configure a new Guest VLAN for this port.
- 802.1x authentication cannot be enabled for a port configured with a Guest VLAN.
- The Guest VLAN function for MAC address authentication does not take effect when port security is enabled.

Related commands: **mac-authentication timer guest-vlan-reauth**.

Examples

Configure VLAN 4 as the Guest VLAN for GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 4
```

mac-authentication max-auth-num

Syntax

mac-authentication max-auth-num *user-number*

undo mac-authentication max-auth-num

View

Ethernet port view

Parameters

user-name: Maximum number of MAC address authentication users allowed to access a port. This argument is in the range of 1 to 256.

Description

Use the **mac-authentication max-auth-num** command to configure the maximum number of MAC address authentication users allowed to access the port. After the number of access users has exceeded the configured maximum number, the switch will not trigger MAC address authentication for subsequent access users, and thus these subsequent access users cannot access the network normally.

Use the **undo mac-authentication max-auth-num** command to restore the maximum number of MAC address authentication users allowed to access the port to the default value.

By default, the maximum number of MAC address authentication users allowed to access a port is 256.

Caution

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port at the same time, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to the Port Security module in this manual for the description on the port security function.
- You cannot configure the maximum number of MAC address authentication users for a port if any user connected to this port is online.

Examples

Set the maximum number of MAC address authentication users allowed to access GigabitEthernet 1/0/2 to 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mac-authentication max-auth-num 100
```

mac-authentication timer guest-vlan-reauth

Syntax

mac-authentication timer guest-vlan-reauth *interval*

undo mac-authentication timer guest-vlan-reauth

View

System view

Parameters

interval: Interval at which the switch re-authenticates users in guest VLANs. This argument is in the range of 1 to 3,600 in seconds.

Description

Use the **mac-authentication timer guest-vlan-reauth** command to configure the interval at which the switch re-authenticates users in guest VLANs. If the user of a port passes the authentication, the port will leave the guest VLAN and return to the initial VLAN configured for it.

Use the **undo mac-authentication timer guest-vlan-reauth** command to restore the re-authentication interval to the default value.

The switch re-authenticates the users in guest VLANs at the interval of 30 seconds by default.

Examples

Configure the switch to re-authenticate users in Guest VLANs at the interval of 60 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-authentication timer guest-vlan-reauth 60
```

Table of Contents

1 IP Address Configuration Commands

IP Address Configuration Commands

display ip interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

If no argument is specified, information about all Layer 3 interfaces is displayed.

Examples

Display information about VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state :UP
Line protocol current state :UP
Internet Address is 192.168.0.39/24 Primary
Broadcast address : 192.168.0.255
The Maximum Transmit Unit : 1500 bytes
IP packets input number: 9678, bytes: 475001, multicasts: 7
IP packets output number: 8622, bytes: 391084, multicasts: 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
```

```
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 1-1 Description on the fields of the **display ip interface** command

Field	Description
current state	Current physical state of the interface, which can be • Administrative DOWN: Indicates that the interface is administratively down; that is, the interface is shut down with the **shutdown** command. • DOWN: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. UP: Indicates that both the administrative and physical states of the interface are up.
Line protocol current state	Current state of the network layer protocol, which can be • DOWN: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface. • UP: Indicates that the protocol state of the interface is up.
Internet Address	IP address of the interface
Broadcast address	Directed broadcast address of the subnet attached to the interface
The Maximum Transmit Unit	Maximum transmission unit on the interface, in bytes
IP packets input number, bytes, multicasts IP packets output number, bytes, multicasts	Total number of packets, bytes, and multicast packets forwarded and received on the interface(the statistics start at the device startup)
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the device startup)

Field	Description
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (the statistics start at the device startup), including the following packets: Echo reply packet, unreachable packet, source quench packet, routing redirect packet, Echo request packet, router advert packet, router solicit packet, time exceed packet, IP header bad packet, timestamp request packet, timestamp reply packet, information request packet, information reply packet, netmask request packet, netmask reply packet, and unknown types of packets.

display ip interface brief

Syntax

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

View

Any view

Parameters

interface-type: Interface type.

interface-number: Interface number.

Description

Use the **display ip interface brief** command to display brief information about a specified or all Layer 3 interfaces.

With no argument included, the command displays information about all layer 3 interfaces; with only the interface type specified, it displays information about all layer 3 interfaces of the specified type; with both the interface type and interface number specified, it displays information about the specified interface.

Related commands: **display ip interface**.

Examples

Display brief information about VLAN-interface 1.

```
<Sysname> display ip interface brief vlan-interface 1
*down: administratively down
(l): loopback
```

```
(s): spoofing
 Interface              IP Address     Physical Protocol     Description
 Vlan-interface1        192.168.0.39   up       up           Vlan-inte...
```

Table 1-2 Description on the fields of the **display ip interface brief** command

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 the interface whose link layer protocol is displayed up may have no such a link present or the link is set up only on demand.
Interface	Interface name
IP Address	IP address of the interface (If no IP address is configured, “unassigned” is displayed.)
Physical	Physical state of the interface, which can be • *down: Indicates that the interface is administratively down; that is, the interface is shut down with the **shutdown** command. • down: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. up: Indicates that both the administrative and physical states of the interface are up.
Protocol	Network layer protocol state of the interface, which can be • down: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface. • up: Indicates that the protocol state of the interface is up.
Description	Interface description information (for detailed information, refer to *VLAN Configuration* and *VLAN Commands*). If the description has no more than 12 characters, the whole description can be displayed. If it has more than 12 characters, only the first nine characters are displayed.

ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* }

undo ip address [*ip-address* { *mask* | *mask-length* }]

View

VLAN interface view, loopback interface view

Parameters

ip-address: IP address, in dotted decimal notation.

mask: Subnet mask, in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask. It is in the range of 0 to 32.

Description

Use the **ip address** command to specify an IP address and mask for a VLAN or loopback interface.

Use the **undo ip address** command to remove an IP address and mask of a VLAN or loopback interface.

By default, no IP address is configured for a VLAN or loopback interface.

Related commands: **display ip interface**.

Examples

Assign the IP address 129.12.0.1 to VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

2 IP Performance Optimization Configuration Commands

IP Performance Optimization Configuration Commands

display fib

Syntax

display fib

View

Any view

Parameters

None

Description

Use the **display fib** command to display all forwarding information base (FIB) information.

Examples

Display all FIB information.

```
<Sysname> display fib
Flag:
  U:Usable   G:Gateway    H:Host       B:Blackhole  D:Dynamic    S:Static
  R:Reject  E:Equal cost multi-path  L:Generated by ARP or ESIS   Destination/Mask  Nexthop
Flag TimeStamp     Interface
10.153.17.0/24     10.153.17.99    U    t[37]          Vlan-interface1
10.153.18.88/32    127.0.0.1       GHU  t[37]          InLoopBack0
10.153.18.0/24     10.153.18.88    U    t[37]          LoopBack0
10.153.17.99/32    127.0.0.1       GHU  t[37]          InLoopBack0
127.0.0.0/8        127.0.0.1       U    t[33]          InLoopBack0
```

Table 2-1 Description on the fields of the **display fib** command

Field	Description
Flag	Flags: U: Usable route. G: Gateway route H: Host route B: Blackhole route D: Dynamic route S: Static route R: Rejected route E: Multi-path equal-cost route L: Route generated by ARP or ESIS
Destination/Mask	Destination address/mask length
Nexthop	Next hop address
TimeStamp	Timestamp
Interface	Forwarding interface

display fib ip-address

Syntax

display fib *ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]

View

Any view

Parameters

ip-address1, ip-address2: Destination IP addresses, in dotted decimal notation. *ip-address1* and *ip-address2* together define an address range. The FIB entries in this address range will be displayed.

mask1, mask2: Subnet masks, in dotted decimal notation.

mask-length1, mask-length2: Lengths of the subnet masks, the number of consecutive ones in the masks, in the range of 0 to 32.

longer: Displays the FIB entries matching the specified address/mask and having masks longer than or equal to the specified mask. If no masks are specified, FIB entries that match the natural network address and have the masks longer than or equal to the natural mask will be displayed.

Description

Use the **display fib** *ip-address* command to view the FIB entries matching 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 and mask will be displayed.

Examples

Display FIB entry information which matches destination 12.158.10.0 and has a mask length no less than eight.

```
<Sysname> display fib 12.158.10.0 longer
  Route Entry Count: 1
Flag:
  U:Usable   G:Gateway    H:Host       B:Blackhole  D:Dynamic    S:Static
  R:Reject   E:Equal cost multi-path   L:Generated by ARP or ESIS
Destination/Mask   Nexthop         Flag TimeStamp     Interface
12.158.10.0/24     12.158.10.1     U    t[85391]      Vlan-interface10
```

Display FIB entry information which has a destination in the range of 12.158.10.0/24 to 12.158.10.6/24 and has a mask length of 24.

```
<Sysname> display fib 12.158.10.0 255.255.255.0 12.158.10.6 255.255.255.0
  Route Entry Count: 1
Flag:
  U:Usable   G:Gateway    H:Host       B:Blackhole  D:Dynamic    S:Static
  R:Reject   E:Equal cost multi-path   L:Generated by ARP or ESIS
Destination/Mask   Nexthop         Flag TimeStamp     Interface
12.158.10.0/24     12.158.10.1     U    t[85391]      Vlan-interface10
```

For details about the displayed information, see Table 2-1.

display fib acl

Syntax

display fib acl *acl-number*

View

Any view

Parameters

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

Description

Use the **display fib acl** command to display the FIB entries matching a specific ACL. For ACL, refer to the part discussing ACL in this manual.

Examples

Configure and display ACL 2001.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 211.71.75.0 0.0.0.255
[Sysname-acl-basic-2001] display acl 2001
Basic ACL  2001, 1 rule
Acl's step is 1
 rule 0 permit source 211.71.75.0 0.0.0.255
```

Display the FIB entries filtered by ACL 2001.

```
<Sysname> display fib acl 2001
Route Entry matched by access-list 2001
  Summary Counts :1
Flag:
  U:Usable   G:Gateway    H:Host       B:Blackhole  D:Dynamic    S:Static
  R:Reject   E:Equal cost multi-path   L:Generated by ARP or ESIS
Destination/Mask   Nexthop         Flag TimeStamp     Interface
211.71.75.0/24     1.1.1.2         GSU  t[250763]     Vlan-interface2
```

For details about the displayed information, see Table 2-1.

display fib |

Syntax

display fib | { **begin** | **exclude** | **include** } *regular-expression*

View

Any view

Parameters

|: Uses a regular expression to match FIB entries. For detailed information about regular expression, refer to *Configuration File Management Command*.

begin: Displays a specific FIB entry and all the FIB entries following it. The specific FIB entry is the first entry that matches the specified regular expression.

exclude: Displays the FIB entries that do not match the specified regular expression.

include: Displays the FIB entries that match the specified regular expression.

regular-expression: A case-sensitive character string.

Description

Use the **display fib** | command to display the FIB entries filtered by the specified regular expression.

Examples

Display the entries starting from the first one containing the string 169.254.0.0.

```
<Sysname> display fib | begin 169.254.0.0
169.254.0.0/16 2.1.1.1      U       t[0]        Vlan-interface1
2.0.0.0/16     2.1.1.1      U       t[0]        Vlan-interface1
```

For details about the displayed information, see Table 2-1.

display fib statistics

Syntax

display fib statistics

View

Any view

Parameters

None

Description

Use the **display fib statistics** command to display the total number of FIB entries.

Examples

Display the total number of FIB entries.

```
<Sysname> display fib statistics
Route Entry Count : 8
```

display icmp statistics

Syntax

display icmp statistics

View

Any view

Parameters

None

Description

Use the **display icmp statistics** command to display the statistics about ICMP packets.

Related commands: **display ip interface**, **reset ip statistics**.

Examples

Display the statistics about ICMP packets.

```
<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 2-2 Description on the fields of the **display icmp statistics** command

Field		Description
Input:	bad formats	Number of received wrong format packets

Field		Description
	bad checksum	Number of received wrong checksum packets
	echo	Number of received echo packets
	destination unreachable	Number of received destination unreachable packets
	source quench	Number of received source quench packets
	redirects	Number of received redirection packets
	echo reply	Number of received replies
	parameter problem	Number of received parameter problem packets
	timestamp	Number of received time stamp packets
	information request	Number of received information request packets
	mask requests	Number of received mask requests
	mask replies	Number of received mask replies
	time exceeded	Number of received expiration packets
Output:	echo	Number of sent echo packets
	destination unreachable	Number of sent destination unreachable packets
	source quench	Number of sent source quench packets
	redirects	Number of sent redirection packets
	echo reply	Number of sent replies
	parameter problem	Number of sent parameter problem packets
	timestamp	Number of sent time stamp packets
	information reply	Number of sent information reply packets
	mask requests	Number of sent mask requests
	mask replies	Number of sent mask replies
	time exceeded	Number of sent expiration packets

display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id socket-id*]

View

Any view

Parameters

socktype *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: ID of a task, in the range 1 to 100.

socket-id: ID of a socket, in the range 0 to 3072.

Description

Use the **display ip socket** command to display socket information.

Examples

Display the TCP socket information.

```
<Sysname> display ip socket socktype 1
SOCK_STREAM:
Task = VTYD(18), 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_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 2, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.56:1161,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 3, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.82:1121,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC
```

Table 2-3 Description on the fields of the **display ip socket** command

Field	Description
SOCK_STREAM	Indicates the socket type is TCP
SOCK_DGRAM	Indicates the socket type is UDP
SOCK_RAW	Indicates the socket type is raw IP
Task	Task ID
socketid	Socket ID
Proto	Protocol number used by the socket, indicating the protocol type that IP carries
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. The value makes sense only for the socket of TCP type, because only TCP is able to cache data.
rb_cc	Current data size in the receiving buffer
socket option	Option of a socket
socket state	State of a socket

display ip statistics

Syntax

display ip statistics

View

Any view

Parameters

None

Description

Use the **display ip statistics** command to display the statistics about IP packets.

Related commands: **display ip interface**, **reset ip statistics**.

Examples

Display the statistics about 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 2-4 Description on the fields of the **display ip statistics** command

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. Unknown protocol packets are destined to the local device, but the upper layer protocol specified in their IP header cannot be processed by the device. (For example, if a switch is not enabled with the Layer 3 multicast function, it considers IGMP packets as unknown protocol packets.)
	bad format	Total number of packets with incorrect header format that contains a wrong version, or has a header length less than 20 bytes.
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option

Field		Description
Output:	forwarding	Total number of IP packets forwarded by the local device
	local	Total number of IP packets initiated from the local device
	dropped	Total number of IP packets discarded
	no route	Total number of IP packets for which no route is available
	compress fails	Total number of IP packets failed to compress
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments discarded
	fragmented	Total number of IP packets successfully fragmented
	couldn't fragment	Total number of IP packets that cannot be fragmented
Reassembling:	sum	Total number of IP packets reassembled
	timeouts	Total number of reassembly timeout IP packets

display tcp statistics

Syntax

display tcp statistics

View

Any view

Parameters

None

Description

Use the **display tcp statistics** command to display the statistics about TCP packets.

Related commands: **display tcp status**, **reset tcp statistics**.

Examples

Display the statistics about TCP connections.

```
<Sysname> display tcp statistics
Received packets:
     Total: 753
     packets in sequence: 412 (11032 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)
```

```
     out-of-order packets: 0 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 481 (8776 bytes)
     duplicate ACK packets: 7, too much ACK packets: 0

Sent packets:
     Total: 665
     urgent packets: 0
     control packets: 5 (including 1 RST)
     window probe packets: 0, window update packets: 2

     data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)
     ACK-only packets: 40 (28 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 2-5 Description on the fields of the **display tcp statistics** command

Field		Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent

Field		Description
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent; in brackets are retransmitted packets
	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: 40	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 keepalive probe failures
Initiated connections		Number of connections initiated
accepted connections		Number of connections accepted
established connections		Number of connections established
Closed connections		Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)
Packets dropped with MD5 authentication		Number of packets dropped by MD5 authentication
Packets permitted with MD5 authentication		Number of packets permitted by MD5 authentication

display tcp status

Syntax

display tcp status

View

Any view

Parameters

None

Description

Use the **display tcp status** command to display the state of all the TCP connections so that you can monitor TCP connections in real time.

Examples

Display the state of all the 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 2-6 Description on the fields of the **display tcp status** command

Field	Description
*	If there is an asterisk before a connection, it means that the TCP connection is authenticated through the MD5 algorithm.
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

display udp statistics

Syntax

display udp statistics

View

Any view

Parameters

None

Description

Use the **display udp statistics** command to display the statistics about UDP packets.

Related commands: **reset udp statistics**.

Examples

Display the statistics about UDP packets.

```
<Sysname> display udp statistics
Received packets:
     Total: 26320
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port: 0
```

```
     total broadcast or multicast packets : 25006
     no socket broadcast or multicast packets: 24989
     not delivered, input socket full: 0
     input packets missing pcb cache: 1314
Sent packets:
     Total: 7187
```

Table 2-7 Description on the fields of the **display udp statistics** command

Field		Description
Received packets:	Total	Total number of received UDP packets
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than header
	data length larger than packet	Number of packets with data longer than packet
	no socket on port	Number of unicast packets with no socket on port
	total broadcast or multicast packets	Total number of received broadcast or multicast packets
	no socket broadcast or multicast packets	Total number of broadcast or multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered due to a full socket cache
	input packets missing pcb cache	Number of packets without matching PCB cache
Sent packets:	Total	Total number of UDP packets sent

icmp redirect send

Syntax

icmp redirect send

undo icmp redirect send

View

System view

Parameters

None

Description

Use the **icmp redirect send** command to enable the device to send ICMP redirection packets.

Use the **undo icmp redirect send** command to disable the device from sending ICMP redirection packets.

By default, the device is enabled to send ICMP redirection packets.

Examples

Disable the device from sending ICMP redirection packets.

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

icmp unreach send

Syntax

icmp unreach send

undo icmp unreach send

View

System view

Parameters

None

Description

Use the **icmp unreach send** command to enable the device to send ICMP destination unreachable packets. After enabled with this feature, the switch, upon receiving a packet with an unreachable destination, discards the packet and then sends a destination unreachable packet to the source host.

Use the **undo icmp unreach send** command to disable the device from sending ICMP destination unreachable packets.

By default, the device is enabled to send ICMP destination unreachable packets.

Examples

Disable the device from sending ICMP destination unreachable packets.

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

reset ip statistics

Syntax

reset ip statistics

View

User view

Parameters

None

Description

Use the **reset ip statistics** command to clear the statistics about IP packets. You can use the **display ip statistics** command to view the current IP packet statistics.

Related commands: **display ip interface**.

Examples

Clear the statistics about IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Parameters

None

Description

Use the **reset tcp statistics** command to clear the statistics about TCP packets. You can use the **display tcp statistics** command to view the current TCP packet statistics.

Examples

Clear the statistics about TCP packets.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Parameters

None

Description

Use the **reset udp statistics** command to clear the statistics about UDP packets. You can use the **display udp statistics** command to view the current UDP packet statistics.

Examples

Clear the statistics about UDP packets.

```
<Sysname> reset udp statistics
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

View

System view

Parameters

time-value: TCP finwait timer, in seconds, in the range 76 to 3600.

Description

Use the **tcp timer fin-timeout** command to configure the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default value of the TCP finwait timer.

By default, the value of the TCP finwait timer is 675 seconds.

When the TCP connection state changes from FIN_WAIT_1 to FIN_WAIT_2, the finwait timer is enabled. If the switch does not receive any FIN packet within the finwait timer interval, the TCP connection will be terminated.

Related commands: **tcp timer syn-timeout**, **tcp window**.

Examples

Configure the value of the TCP finwait timer as 800 seconds.

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

Parameters

time-value: TCP synwait timer, in seconds, in the range 2 to 600.

Description

Use the **tcp timer syn-timeout** command to configure the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default value of the TCP synwait timer.

By default, the value of the TCP synwait timer is 75 seconds.

When sending a SYN packet, TCP starts the synwait timer. If no response packet is received within the synwait timer interval, the TCP connection will be terminated.

Related commands: **tcp timer fin-timeout**, **tcp window**.

Examples

Configure the value of the TCP synwait timer as 80 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Parameters

window-size: Size of the send/receive buffer, in kilobytes (KB), in the range of 1 to 32.

Description

Use the **tcp window** command to configure the size of the TCP send/receive buffer,.

Use the **undo tcp window** command to restore the default.

By default, the size of the TCP send/receive buffer is 8 KB.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Examples

Configure the size of the TCP send/receive buffer as 3 KB.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tcp window 3
```

Table of Contents

1 DHCP Relay Agent Configuration Commands

DHCP Relay Agent Configuration Commands

address-check

Syntax

address-check enable

address-check disable

View

VLAN interface view

Parameters

None

Description

Use the **address-check enable** command to enable IP address match checking on the DHCP relay agent. After this feature is enabled, the DHCP relay agent can cooperate with the ARP module to check whether a requesting client's IP and MAC addresses match a binding on the DHCP relay agent; if not, the client cannot access outside networks via the DHCP relay agent.

Use the **address-check disable** command to disable IP address match checking on the DHCP relay agent.

By default, IP address match checking on the DHCP relay agent is disabled.

Examples

Enter system view.

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

Enter VLAN-interface 1 view.

```
[Sysname] interface vlan-interface 1
```

Enable IP address match checking on VLAN-interface 1 of the DHCP relay agent.

```
[Sysname-Vlan-interface1] address-check enable
```

dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

View

System view

Parameters

None

Description

Use the **dhcp relay information enable** command to enable Option 82 support on a DHCP relay agent.

Use the **undo dhcp relay information enable** command to disable Option 82 support on a DHCP relay agent.

By default, this function is disabled.

 **Note**

By default, with the Option 82 support function enabled on the DHCP relay agent, the DHCP relay agent will adopt the **replace** strategy to process the request packets containing Option 82. However, if other strategies are configured before, then enabling the 82 supporting on the DHCP relay will not change the configured strategies.

Related commands: **dhcp relay information strategy**.

Examples

Enter system view.

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

Enable Option 82 support on a DHCP relay agent.

```
[Sysname] dhcp relay information enable
```

dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View

System view

Parameters

drop: Specifies to drop messages containing Option 82.

keep: Specifies to forward messages containing Option 82 without any change.

replace: Specifies to forward messages containing Option 82 after replacing the original Option 82 with the Option 82 padded with the specified content.

Description

Use the **dhcp relay information strategy** command to configure the DHCP relay agent handling strategy for messages containing Option 82 sent by the DHCP client.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

By default, the handling strategy for messages containing Option 82 is **replace**.

Related commands: **dhcp relay information enable**.

Examples

Enter system view.

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

Configure the DHCP relay agent handling strategy for messages containing Option 82 sent by the DHCP client as **drop**.

```
[Sysname] dhcp relay information strategy drop
```

dhcp-security static

Syntax

dhcp-security static *ip-address mac-address*

undo dhcp-security { *ip-address* | **all** | **dynamic** | **static** }

View

System view

Parameters

ip-address: User IP address.

mac-address: User MAC address.

all: Removes all user address entries.

dynamic: Removes dynamic user address entries.

static: Removes static user address entries.

Description

Use the **dhcp-security static** command to configure a static DHCP address binding entry.

Use the **undo dhcp-security** command to remove one or all address binding entries, or all address binding entries of a specified type.

Related commands: **display dhcp-security**.

Examples

Enter system view.

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

Configure a static address binding entry, with the IP address being 1.1.1.1 and the MAC address being 0005-5D02-F2B3.

```
[Sysname] dhcp-security static 1.1.1.1 0005-5D02-F2B3
```

dhcp-server

Syntax

dhcp-server *groupNo*

undo dhcp-server

View

VLAN interface view

Parameters

groupNo: DHCP server group number. This argument ranges from 0 to 19.

Description

Use the **dhcp-server** command to map the current VLAN interface to a DHCP server group.

Use the **undo dhcp-server** command to cancel the mapping.

Note that:

- A DHCP server group can correspond to multiple interfaces, while an interface can only be correlated with one DHCP server group.
- If you execute the **dhcp-server** command repeatedly, the latest configuration will overwrite the previous one.
- Before referencing a DHCP server group, you need to use the **dhcp-server** *groupNo* **ip** *ip-address*&<1-8> command to configure the DHCP server group.

Related commands: **dhcp-server ip**, **display dhcp-server**, **display dhcp-server interface vlan-interface**.

Note

To improve security and avoid malicious attack to the unused SOCKETs, S4200G Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows.

- When a VLAN interface is mapped to a DHCP server group with the **dhcp-server** command, the DHCP relay agent is enabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are enabled.
- When the mapping between a VLAN interface and a DHCP server group is removed with the **undo dhcp-server** command, DHCP services are disabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are disabled.

Examples

Enter system view.

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

Enter VLAN-interface 1 view.

```
[Sysname] interface vlan-interface 1
```

Specify that VLAN-interface 1 corresponds to DHCP server group 1.

```
[Sysname-Vlan-interface1] dhcp-server 1
```

dhcp-server detect

Syntax

dhcp-server detect

undo dhcp-server detect

View

System view

Parameters

None

Description

Use the **dhcp-server detect** command to enable the switch serving as a DHCP relay agent to detect unauthorized DHCP servers.

Use the **undo dhcp-server detect** command to disable the unauthorized DHCP server detection function.

By default, the unauthorized DHCP server detection function is disabled

Related commands: **dhcp server**, **display dhcp-server**.

Examples

Enter system view

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

Enable the unauthorized-DHCP server detection function on the DHCP relay agent.

```
[Sysname] dhcp-server detect
```

dhcp-server ip

Syntax

dhcp-server *groupNo* **ip** *ip-address*&<1-8>

undo dhcp-server *groupNo*

View

System view

Parameters

groupNo: DHCP server group number, ranging from 0 to 19.

ip-address&<1-8>: IP address of the DHCP server. &<1-8> indicates that up to eight IP addresses can be input, with any two IP addresses separated by a space.

Description

Use the **dhcp-server ip** command to configure the DHCP server IP address(es) in a specified DHCP server group.

Use the **undo dhcp-server** command to remove all DHCP server IP addresses in a DHCP server group.

Related commands: **dhcp-server**, **display dhcp-server**.

Examples

Enter system view.

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

Configure three DHCP server IP addresses 1.1.1.1, 2.2.2.2, and 3.3.3.3 for DHCP server group 1, so that this group contains three DHCP servers (server 1, server 2 and server 3).

```
[Sysname] dhcp-server 1 ip 1.1.1.1 2.2.2.2 3.3.3.3
```

display dhcp-security

Syntax

display dhcp-security [*ip-address* | **dynamic** | **static**]

View

Any view

Parameters

ip-address: IP address. This argument is used to display the user address entry with the specified IP address.

dynamic: Displays the dynamic user address entries.

static: Displays the static user address entries.

Description

Use the **display dhcp-security** command to display information about address binding entries on the DHCP relay agent.

Examples

Display information about all address binding entries.

```
<Sysname> display dhcp-security
 IP Address      MAC Address     IP Address Type
 10.1.1.1        0001-0001-0001  Static
 192.168.10.2    000d-88f7-b090  Dynamic_ack
---   2 dhcp-security item(s)  found   ---
```

Table 1-1 Description on the fields of the **display dhcp-security** command

Field	Description
IP Address	IP address of the DHCP client
MAC Address	MAC address of the DHCP client
IP Address Type	Type of the user address entry (static/dynamic)

display dhcp-server

Syntax

display dhcp-server *groupNo*

View

Any view

Parameters

groupNo: DHCP server group number, ranging from 0 to 19.

Description

Use the **display dhcp-server** command to display information about a specified DHCP server group.

Related commands: **dhcp-server ip**, **dhcp-server**, **display dhcp-server interface vlan-interface**.

Examples

Display information about DHCP server group 0.

```
<Sysname> display dhcp-server 0
 IP address of DHCP server group 0:         1.1.1.1
 IP address of DHCP server group 0:         2.2.2.2
 IP address of DHCP server group 0:         3.3.3.3
 IP address of DHCP server group 0:         4.4.4.4
 IP address of DHCP server group 0:         5.5.5.5
 IP address of DHCP server group 0:         6.6.6.6
 IP address of DHCP server group 0:         7.7.7.7
 IP address of DHCP server group 0:         8.8.8.8
 Messages from this server group: 0
 Messages to this server group: 0
 Messages from clients to this server group: 0
 Messages from this server group to clients: 0
 DHCP_OFFER messages: 0
 DHCP_ACK messages: 0
 DHCP_NAK messages: 0
 DHCP_DECLINE messages: 0
 DHCP_DISCOVER messages: 0
 DHCP_REQUEST messages: 0
 DHCP_INFORM messages: 0
 DHCP_RELEASE messages: 0
 BOOTP_REQUEST messages: 0
```

```
BOOTP_REPLY messages: 0
```

Table 1-2 Description on the fields of the **display dhcp-server** command

Field	Description
IP address of DHCP server group 0:	DHCP server IP addresses of DHCP server group 0
Messages from this server group	Number of the packets the DHCP relay receives from the DHCP server group
Messages to this server group	Number of the packets the DHCP relay sends to the DHCP server group
Messages from clients to this server group	Number of the packets the DHCP relay receives from the DHCP clients
Messages from this server group to clients	Number of the packets the DHCP relay sends to the DHCP clients
DHCP_OFFER messages	Number of the DHCP-OFFER packets received by the DHCP relay
DHCP_ACK messages	Number of the DHCP-ACK packets received by the DHCP relay
DHCP_NAK messages	Number of the DHCP-NAK packets received by the DHCP relay
DHCP_DECLINE messages	Number of the DHCP-DECLINE packets received by the DHCP relay
DHCP_DISCOVER messages	Number of the DHCP-DISCOVER packets received by the DHCP relay
DHCP_REQUEST messages	Number of the DHCP-REQUEST packets received by the DHCP relay
DHCP_INFORM messages	Number of the DHCP-INFORM packets received by the DHCP relay
DHCP_RELEASE messages	Number of the DHCP-RELEASE packets received by the DHCP relay
BOOTP_REQUEST messages	Number of the BOOTP request packets
BOOTP_REPLY messages	Number of the BOOTP response packets

display dhcp-server interface

Syntax

display dhcp-server interface Vlan-interface *vlan-id*

View

Any view

Parameters

vlan-id: VLAN ID.

Description

Use the **display dhcp-server interface** command to display information about the DHCP server group to which a VLAN interface is mapped.

Related commands: **dhcp-server**, **display dhcp-server**.

Examples

Display information about the DHCP server group to which VLAN-interface 2 is mapped.

```
<Sysname> display dhcp-server interface vlan-interface 2
 Dhcp-group 0 is configured on this interface
```

The above information indicates the VLAN-interface 2 is mapped to DHCP server group 0.

reset dhcp-server

Syntax

reset dhcp-server *groupNo*

View

User view

Parameters

groupNo: DHCP server group number, ranging from 0 to 19.

Description

Use the **reset dhcp-server** command to clear the statistics information of the specified DHCP server group.

Related commands: **dhcp server**, **display dhcp-server**.

Examples

Clear the statistics information of DHCP server group 2.

```
<Sysname> reset dhcp-server 2
```

2 DHCP Snooping Configuration Commands

DHCP Snooping Configuration Commands

dhcp-snooping

Syntax

dhcp-snooping

undo dhcp-snooping

View

System view

Parameters

None

Description

Use the **dhcp-snooping** command to enable the DHCP snooping function.

Use the **undo dhcp-snooping** command to disable the DHCP snooping function. After DHCP snooping is disabled, all the ports can forward DHCP replies from the DHCP server without recording the IP-to-MAC bindings of the DHCP clients.

By default, the DHCP snooping function is disabled.

Note that:

- You need to disable DHCP relay agent before enabling DHCP snooping on the switch.
- The clients connected to a DHCP snooping device cannot obtain an IP address through BOOTP.

Related commands: **display dhcp-snooping**.

Examples

Enter system view.

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

Enable the DHCP snooping function.

```
[Sysname] dhcp-snooping
```

dhcp-snooping information enable

Syntax

dhcp-snooping information enable

undo dhcp-snooping information enable

View

System view

Parameters

None

Description

Use the **dhcp-snooping information enable** command to enable DHCP snooping Option 82.

Use the **undo dhcp-snooping information enable** command to disable DHCP snooping Option 82.

DHCP snooping Option 82 is disabled by default.

Enable DHCP snooping before performing this configuration.

Examples

Enable DHCP snooping Option 82.

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

dhcp-snooping information format

Syntax

dhcp-snooping information format { **hex** | **ascii** }

View

System view

Parameters

hex: Specifies the storage format of Option 82 as HEX (namely, hexadecimal string).

ascii: Specifies the storage format of Option 82 as ASCII.

Description

Use the **dhcp-snooping information format** command to configure the storage format of non-user-defined Option 82 as HEX or ASCII.

By default, the Option 82 is in HEX format.

Note

The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the storage format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.

Examples

Configure the storage format of Option 82 as ASCII.

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

dhcp-snooping information packet-format

Syntax

dhcp-snooping information packet-format { **extended** | **standard** }

View

System view

Parameters

extended: Specifies the padding format for Option 82 as the extended format.

standard: Specifies the padding format for Option 82 as the standard format.

Description

Use the **dhcp-snooping information packet-format** command to configure the padding format for Option 82 as the extended or standard one.

By default, the padding format for Option 82 is the extended one.

Examples

Configure the padding format for Option 82 as the standard one.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dhcp-snooping information packet-format standard
```

dhcp-snooping information remote-id

Syntax

dhcp-snooping information remote-id { **sysname** | **string** *string* }

undo dhcp-snooping information remote-id

View

System view

Parameters

sysname: Uses the system name (sysname) of the DHCP snooping device to pad the remote ID sub-option in Option 82.

string: Customized content of the remote ID sub-option, a string of 1 to 63 ASCII characters.

Description

Use the **dhcp-snooping information remote-id** command to configure the remote ID sub-option in Option 82.

Use the **undo dhcp-snooping information remote-id** command to restore the default value of the remote ID sub-option in Option 82.

By default, the remote ID sub-option in Option 82 is the MAC address of the DHCP Snooping device that received the DHCP client's request.

Examples

Configure the remote ID sub-option of Option 82 as the system name (sysname) of the DHCP snooping device.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dhcp-snooping information remote-id sysname
```

dhcp-snooping information strategy

Syntax

dhcp-snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp-snooping information strategy

View

System view, Ethernet port view

Parameters

drop: If a packet contains Option 82, DHCP snooping drops this packet.

keep: If a packet contains Option 82, DHCP snooping keeps and forwards this packet.

replace: If a packet contains Option 82, DHCP snooping replaces the original Option 82 field with the Option 82 field having the specified padding content and forwards the packet.

Description

Use the **dhcp-snooping information strategy** command in system view to configure a handling policy for DHCP requests that contain Option 82 sent by the DHCP client.

Use the **undo dhcp-snooping information strategy** command to restore the default handling policy.

Use the **dhcp-snooping information strategy** command in Ethernet port view to configure a handling policy for requests that contain Option 82 received on the current port.

Use the **undo dhcp-snooping information strategy** command to restore the default handling policy.

By default, after DHCP-snooping Option 82 support is enabled, DHCP snooping replaces the Option 82 field in the requests sent by the DHCP clients.

Caution

- Enable DHCP-snooping and DHCP-snooping Option 82 before performing this configuration.
- If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Examples

Configure the **keep** handling policy for DHCP requests that contain Option 82 on the DHCP snooping device.

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

dhcp-snooping information vlan circuit-id

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string** *string*

undo dhcp-snooping information { [**vlan** *vlan-id*] **circuit-id** | **circuit-id all** }

View

Ethernet port view

Parameters

vlan *vlan-id*: Specifies a VLAN. DHCP packets from the VLAN are padded with the circuit ID sub-option.

string: Content of the circuit ID sub-option, a string of 3 to 63 ASCII characters.

Description

Use the **dhcp-snooping information vlan circuit-id** command to configure the content of the circuit ID field in Option 82.

Use the **undo dhcp-snooping information circuit-id** command to restore the default.

With **vlan** *vlan-id* specified, the customized circuit ID sub-option applies only to the DHCP packets from the specified VLAN. With no **vlan** *vlan-id* specified, the customized circuit ID sub-option applies to all DHCP packets that pass through the current port.

Use the **undo dhcp-snooping information vlan** *vlan-id* **circuit-id** command to restore the default circuit ID in DHCP packets from the specified VLAN.

Use the **undo dhcp-snooping information circuit-id** command to restore the default circuit ID for all DHCP packets except those from the specified VLAN.

Use the **undo dhcp-snooping information circuit-id all** command to restore the default circuit ID for all DHCP packets.

By default, the circuit ID field in Option 82 contains the VLAN ID and index of the port that received the client's request.

If you have configured a circuit ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.

Examples

Set the circuit ID field in Option 82 of the DHCP messages sent through GigabitEthernet 1/0/1 to **abc**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id string abc
```

dhcp-snooping information vlan remote-id

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **remote-id string** *string*

undo dhcp-snooping information { [**vlan** *vlan-id*] **remote-id** | **remote-id all** }

View

Ethernet port view

Parameters

vlan *vlan-id*: Specifies the VLAN ID of the remote ID to be customized.

string: Customized content of the remote ID sub-option, a string of 3 to 63 ASCII characters.

Description

Use the **dhcp-snooping information vlan remote-id** command to configure the content of the remote ID in Option 82

Use the **undo dhcp-snooping information remote-id** command to restore the default remote ID in Option 82.

With **vlan** *vlan-id* specified, the customized remote ID sub-option applies only to the DHCP packets from the specified VLAN. Without **vlan** *vlan-id* specified, the customized remote ID sub-option applies to all DHCP packets that pass through the current port.

Use the **undo dhcp-snooping information vlan** *vlan-id* **remote-id** command to restore the default remote ID in DHCP packets from the specified VLAN.

Use the **undo dhcp-snooping information remote-id** command to restore the default remote ID in all DHCP packets except those from the specified VLAN.

Use the **undo dhcp-snooping information remote-id all** command to restore the default remote ID in all DHCP packets.

By default, the remote ID sub-option in Option 82 is the MAC address of the DHCP Snooping device that received the DHCP client's request.

If you have configured a remote ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.

Examples

Configure the remote ID of Option 82 in DHCP packets to **abc** on the port GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id string abc
```

dhcp-snooping trust

Syntax

dhcp-snooping trust

undo dhcp-snooping trust

View

Ethernet port view

Parameters

None

Description

Use the **dhcp-snooping trust** command to set an Ethernet port to a DHCP-snooping trusted port.

Use the **undo dhcp-snooping trust** command to restore an Ethernet port to a DHCP-snooping untrusted port.

By default, with the DHCP snooping enabled, all the ports of a switch are untrusted ports.

Note that:

After DHCP snooping is enabled, you need to specify the port connected to a valid DHCP server as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the ports connected to DHCP clients must be in the same VLAN.

Related commands: **display dhcp-snooping trust**.

Examples

Enter system view.

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

Set the GigabitEthernet 1/0/1 port to a trusted port.

```
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping trust
```

display dhcp-snooping

Syntax

display dhcp-snooping [**unit** *unit-id*]

View

Any view

Parameters

unit *unit-id:* Displays the DHCP-snooping information on the specified device, the value is 1 for S4200G series switches.

Description

Use the **display dhcp-snooping** command to display the user IP-MAC address mapping entries recorded by the DHCP snooping function.

Related commands: **dhcp-snooping**.

Examples

Display the user IP-MAC address mapping entries recorded by the DHCP snooping function.

```
<Sysname> display dhcp-snooping
 DHCP-Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Unit ID : 1
 Type IP Address     MAC Address      Lease      VLAN Interface

 ==== ============= ============== ========= ==== ================

 D    10.1.1.1        000f-e200-0006   200      1    GigabitEthernet1/0/1
---   1 dhcp-snooping item(s) of unit 1 found   ---
```

display dhcp-snooping trust

Syntax

display dhcp-snooping trust

View

Any view

Parameters

None

Description

Use the **display dhcp-snooping trust** command to display the (enabled/disabled) state of the DHCP snooping function and the trusted ports.

Related commands: **dhcp-snooping trust**.

Examples

Display the state of the DHCP snooping function and the trusted ports.

```
<Sysname> display dhcp-snooping trust
 DHCP-Snooping is enabled.
 DHCP-Snooping trust become effective.
 Interface                Trusted
 ==================== ================
 GigabitEthernet1/0/10     Trusted
```

The above display information indicates that the DHCP snooping function is enabled, and the GigabitEthernet 1/0/10 port is a trusted port.

display ip source static binding

Syntax

display ip source static binding [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

View

Any view

Parameters

vlan-id: ID of the VLAN whose IP static binding entries are to be displayed.

interface-type interface-number: Type and number of the port whose IP static binding entries are to be displayed.

Description

Use the **display ip source static binding** command to display the IP static binding entries configured. If you specify a VLAN, all the IP static binding entries for the specified VLAN will be displayed. If you specify a port, all the IP static binding entries for the specified port will be displayed.

Examples

Display all IP static binding entries configured.

```
<Sysname> display ip source static binding
 Type IP Address      MAC Address     Remaining  VLAN Interface
                                      lease
 ==== =============== =============== =========  ==== =================
 S    192.168.0.25    0015-e20f-0101  infinit     1    GigabitEthernet1/0/2
 S    192.168.0.58    0001-e201-4f01  infinit     1    GigabitEthernet1/0/3
 S    192.168.0.101   000f-0101-0204  infinit     1    GigabitEthernet1/0/2
 S    192.168.0.122   000f-e20f-21a3  infinit     1    GigabitEthernet1/0/3
 S    192.168.0.144   0015-e943-712f  infinit     1    GigabitEthernet1/0/2
---   5 static binding item(s) found   ---
```

ip check dot1x enable

Syntax

ip check dot1x enable

undo ip check dot1x enable

View

Ethernet port view

Parameters

None

Description

Use the **ip check dot1x enable** command to enable IP filtering based on IP-to-MAC mappings of authenticated 802.1x clients.

Use the **undo ip check dot1x enable** command to disable the function.

By default, IP filtering based on IP-to-MAC mappings of authenticated 802.1x clients is disabled.

Note that the **ip check dot1x enable** and the **ip check source ip-address mac-address** commands are mutually exclusive.

Examples

Enable IP filtering based on IP-to-MAC mappings of authenticated 802.1x clients on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/2
[Sysname-GigabitEthernet1/0/2] ip check dot1x enable
```

ip check source ip-address

Syntax

ip check source ip-address [**mac-address**]

undo ip check source ip-address [**mac-address**]

View

Ethernet port view

Parameters

mac-address: Enables IP filtering based on the source MAC address of the packets.

Description

Use the **ip check source ip-address** command to enable the filtering of the IP packets received through the current port based on the source IP address of the packets.

Use the **undo ip check source ip-address** command to disable the filtering of the IP packets received through the current port based on the source IP address of the packets.

Use the **ip check source ip-address mac-address** command to enable the filtering of the IP packets received through the current port based on the source IP address and source MAC address of the packets.

Use the **undo ip check source ip-address mac-address** command to disable the filtering of the IP packets received through the current port based on the source IP address and source MAC address of the packets.

By default, the filtering of the IP packets received through a port based on the source IP address or source MAC address of the packets is disabled.

Examples

Enable the filtering of the IP packets received through port GigabitEthernet 1/0/11 based on the source IP address of the packets.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet1/0/11
[Sysname-GigabitEthernet1/0/11] ip check source ip-address
```

ip source static binding

Syntax

ip source static binding ip-address *ip-address* [**mac-address** *mac-address*]

undo ip source static binding ip-address *ip-address*

View

Ethernet port view

Parameters

ip-address *ip-address*: Specifies the IP address to be statically bound.

mac-address *mac-address*: Specifies the MAC address to be statically bound.

Description

Use the **ip source static binding ip-address** command to configure the static binding among source IP address, source MAC address, and the port number so as to generate static binding entries.

Use the **undo ip source static binding ip-address** command to remove the static binding among source IP address, source MAC address, and the port.

By default, no binding among source IP address, source MAC address, and the port number is configured.

To create a static binding after IP filtering is enabled with the **mac-address** keyword included on a port, the *mac-address* argument must be specified; otherwise, the packets sent from this IP address cannot pass the IP filtering.

Related commands: **ip check source ip-address**.

Examples

Configure static binding among source IP address 1.1.1.1, source MAC address 0015-e20f-0101, and GigabitEthernet 1/0/3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet1/0/3
[Sysname-GigabitEthernet1/0/3] ip source static binding ip-address 1.1.1.1 mac-address
0015-e20f-0101
```

reset dhcp-snooping

Syntax

reset dhcp-snooping [*ip-address*]

View

User view

Parameters

ip-address: IP address of a DHCP snooping entry to be deleted.

Description

Use the **reset dhcp-snooping** command to remove DHCP snooping entries from a switch. If no *ip-address* is specified, all DHCP snooping entries are removed.

Examples

Remove all DHCP snooping entries from the switch.

```
<Sysname> reset dhcp-snooping
```

3 Rate Limit Configuration Commands

Rate Limit Configuration Commands

dhcp protective-down recover enable

Syntax

dhcp protective-down recover enable

undo dhcp protective-down recover enable

View

System view

Parameters

None

Description

Use the **dhcp protective-down recover enable** command to enable port state auto-recovery on the switch.

Use the **undo dhcp protective-down recover enable** command to disable port state auto-recovery.

With the port state auto-recovery function, a port that is shut down because the DHCP traffic rate limit configured on it is exceeded can automatically be brought up after a specified interval.

By default, the port state auto-recovery function on the switch is disabled.

Examples

Enable port state auto-recovery on the switch.

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

dhcp protective-down recover interval

Syntax

dhcp protective-down recover interval *interval*

undo dhcp protective-down recover interval

View

System view

Parameters

interval: Interval (in seconds) for a port disabled due to the DHCP traffic exceeding the set threshold to be brought up again. This argument ranges from 10 to 86,400.

Description

Use the **dhcp protective-down recover interval** command to set an auto recovery interval.

Use the **undo dhcp protective-down recover interval** command to restore the default interval.

With the port state auto-recovery function enabled on a switch, the auto recovery interval defaults to 300 seconds.

Note that:

- Before configuring the port state auto-recovery interval, you must enable port state auto-recovery on the switch first.
- The new port state auto-recovery interval only applies to the ports that are shut down after the **dhcp protective-down recover interval** command is last executed.

Examples

Set the port state auto-recovery interval to 30 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dhcp protective-down recover enable
[Sysname] dhcp protective-down recover interval 30
```

dhcp rate-limit

Syntax

dhcp rate-limit *rate*

undo dhcp rate-limit

View

Ethernet port view

Parameters

rate: Maximum rate of DHCP traffic in pps. This argument ranges from 10 to 150.

Description

Use the **dhcp rate-limit** command to configure the maximum rate of DHCP traffic for the port. When the number of DHCP packets received on the port per second exceeds the specified threshold, the switch will discard the exceeding DHCP packets.

Use the **undo dhcp rate-limit** command to restore the default.

By default, after the DHCP traffic limit is enabled, the maximum rate of DHCP traffic is 15 pps.

Note that:

You need to enable the function to limit DHCP traffic (refer to the **dhcp rate-limit enable** command) for a port before executing either of these two commands for the port.

Examples

Configure the DHCP traffic threshold to 100 pps for port GigabitEthernet 1/0/11.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] dhcp rate-limit enable
[Sysname-GigabitEthernet1/0/11] dhcp rate-limit 100
```

dhcp rate-limit enable

Syntax

dhcp rate-limit enable

undo dhcp rate-limit enable

View

Ethernet port view

Parameters

None

Description

Use the **dhcp rate-limit enable** command to enable the function to limit DHCP traffic for an Ethernet port. You can use this command to limit the DHCP traffic passing through an Ethernet port. When the number of DHCP packets received on the port per second exceeds the specified threshold (the default value is 15 pps), the switch will discard the exceeding DHCP packets.

Use the **undo dhcp rate-limit enable** command to disable the function. You can use this command to relieve the DHCP traffic limit configured on an Ethernet port.

By default, the function to limit DHCP traffic is disabled on an Ethernet port. That is, DHCP traffic passing through an Ethernet port is not limited.

Examples

Enable the function to limit DHCP traffic for GigabitEthernet 1/0/11 port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] dhcp rate-limit enable
```

4 DHCP/BOOTP Client Configuration

DHCP Client Configuration Commands

display dhcp client

Syntax

display dhcp client [**verbose**]

View

Any view

Parameters

verbose: Displays the detailed address allocation information.

Description

Use the **display dhcp client** command to display the information about the address allocation of DHCP clients.

Note that S4200G series Ethernet switches that operate as DHCP clients support a maximum lease duration of 24 days currently.

Examples

Display the information about the address allocation of DHCP clients.

```
<Sysname> display dhcp client verbose
DHCP client statistic information:
Vlan-interface1:
Current machine state: BOUND
Allocated IP: 192.168.0.2 255.255.255.0
Allocated lease: 86400 seconds, T1: 43200 seconds, T2: 75600 seconds
Lease from 2002.09.20 01:05:03   to   2002.09.21 01:05:03
Server IP: 192.168.0.1
Transaction ID = 0x3d8a7431
Default router: 192.168.0.1
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.
```

Table 4-1 Description on the fields of the **display dhcp client** command

Field	Description
Vlan-interface1	VLAN interface operating as a DHCP client to obtain an IP address dynamically
Current machine state	The state of the client state machine
Allocated IP	IP address allocated to the DHCP client
lease	Lease period
T1	Renewal timer setting
T2	Rebinding timer setting
Lease from….to….	The starting and end time of the lease period
Server IP	IP address of the DHCP server selected
Transaction ID	Transaction ID
Default router	Gateway address
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.	The timer expires in 11 hours, 56 minutes, and 1 second.

ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

View

VLAN interface view

Parameters

None

Description

Use the **ip address dhcp-alloc** command to configure a VLAN interface to obtain an IP address through DHCP.

Use the **undo ip address dhcp-alloc** command to cancel the configuration.

By default, a VLAN interface does not use DHCP to obtain an IP address.

Note

To improve security and avoid malicious attacks to the unused sockets, S4200G Ethernet switches provide the following functions:

- UDP ports 67 and 68 used by DHCP are enabled/disabled only when DHCP is enabled/disabled.

The implementation is as follows:

- After the DHCP client is enabled by executing the **ip address dhcp-alloc** command, UDP port 68 is enabled.
- After the DHCP client is disabled by executing the **undo ip address dhcp-alloc** command, UDP port 68 is disabled.

Examples

Configure VLAN-interface 1 to obtain an IP address through DHCP.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```

BOOTP Client Configuration Commands

display bootp client

Syntax

display bootp client [**interface Vlan-interface** *vlan-id*]

View

Any view

Parameters

vlan-id: ID of the VLAN interface.

Description

Use the **display bootp client** command to display BOOTP client-related information, including the MAC address of the BOOTP client and the IP address obtained.

Examples

Display the BOOTP client-related information.

```
<Sysname> display bootp client interface Vlan-interface 1
Vlan-interface1:
Allocated IP: 192.168.0.2 255.255.255.0
Transaction ID = 0x3d8a7431
Mac Address  000f-e20a-c3ef
Default router: 192.168.0.1
```

Table 4-2 Description on the fields of the **display bootp client** command

Field	Description
Vlan-interface1	VLAN-interface 1 is configured to obtain an IP address through BOOTP.
Allocated IP	IP address allocated to the VLAN interface
Transaction ID	Value of the XID field in BOOTP packets

Field	Description
Mac Address	MAC address of the BOOTP client
Default router	Default router

ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

View

VLAN interface view

Parameters

None

Description

Use the **ip address bootp-alloc** command to configure a VLAN interface to obtain an IP address through BOOTP.

Use the **undo ip address bootp-alloc** command to cancel the configuration.

By default, a VLAN interface does not use BOOTP to obtain an IP address.

Related commands: **display bootp client**.

Examples

Configure VLAN-interface 1 to obtain an IP address through BOOTP.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address bootp-alloc
```

Table of Contents

1 ACL Configuration Commands

ACL Configuration Commands

acl

Syntax

acl number *acl-number* [**match-order** { **auto** | **config** }]

undo acl { **all** | **number** *acl-number* }

View

System view

Parameters

all: Specifies to remove all access control lists (ACLs).

number *acl-number*: Specifies the number of an existing ACL or an ACL to be defined. ACL number identifies the type of an ACL as follows.

- An ACL number in the range 2000 to 2999 identifies a basic ACL.
- An ACL number in the range 3000 to 3999 identifies an advanced ACL. Note that 3998 and 3999 cannot be configured because they are reserved for cluster management.
- An ACL number in the range 4000 to 4999 identifies a layer 2 ACL.
- An ACL number in the range 5000 to 5999 identifies an IPv6 ACL.

match-order: Specifies the match order for ACL rules. Following two match orders exist.

- **auto**: Specifies to match ACL rules according to the depth-first rule.
- **config**: Specifies to match ACL rules in the order they are defined.

Note that the **match-order** keyword is not available to Layer 2 ACLs and IPv6 ACLs. The match order for layer 2 ACLs and IPv6 ACLs can only be **config**. For details about the two match orders, refer to the relevant description in *ACL Operation*.

Description

Use the **acl** command to define an ACL and enter the corresponding ACL view.

Use the **undo acl** command to remove all the rules of the specified ACL or all the ACLs.

By default, ACL rules are matched in the order they are defined.

Only after the rules in an existing ACL are fully removed can you modify the match order of the ACL.

In ACL view, you can use the **rule** command to add rules to the ACL.

Related commands: **rule**.

Examples

Define ACL 2000 and specify “depth-first” as the match order.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] acl number 2000 match-order auto
[Sysname-acl-basic-2000]
```

Add three rules with different numbers of zeros in the source wildcards.

```
[Sysname-acl-basic-2000] rule 1 permit source 1.1.1.1 0.255.255.255
[Sysname-acl-basic-2000] rule 2 permit source 2.2.2.2 0.0.255.255
[Sysname-acl-basic-2000] rule 3 permit source 3.3.3.3 0.0.0.255
```

Use the **display acl** command to display the configuration information of ACL 2000.

```
[Sysname-acl-basic-2000] display acl 2000
Basic ACL  2000, 3 rules, match-order is auto
Acl's step is 1
 rule 3 permit source 3.3.3.0 0.0.0.255
 rule 2 permit source 2.2.0.0 0.0.255.255
 rule 1 permit source 1.0.0.0 0.255.255.255
```

As shown in the output information, the switch sorts the rules of ACL 2000 in the depth-first order: a rule with more zeros in the source IP address wildcard has a higher priority.

description

Syntax

description *text*

undo description

View

Basic ACL view, advanced ACL view, Layer 2 ACL view, IPv6 ACL view

Parameters

text: Description string to be assigned to an ACL, a string of 1 to 127 characters. Blank spaces and special characters are acceptable.

Description

Use the **description** command to assign a description string to an ACL.

Use the **undo description** to remove the description string of the ACL.

You can give ACLs descriptions to provide relevant information such as their application purposes and the ports they are applied to, so that you can easily identity and distinguish ACLs by their descriptions.

By default, no description string is assigned for an ACL.

Examples

Assign description string “This ACL is used for filtering all HTTP packets” to ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This ACL is used for filtering all HTTP packets
```

Use the **display acl** command to view the configuration information of ACL 3000.

```
[Sysname-acl-adv-3000] display acl 3000
Advanced ACL  3000, 0 rule
```

```
This acl is used for filtering all HTTP packets
Acl's step is 1
```

Remove the description string of ACL 3000.

```
[Sysname-acl-adv-3000] undo description
```

display acl

Syntax

display acl { **all** | *acl-number* }

View

Any view

Parameters

all: Displays all ACLs.

acl-number: Number of the ACL to be displayed, in the range of 2000 to 5999.

Description

Use the **display acl** command to display the configuration information of a specified or all ACLs.

Note that if you specify the match order of an ACL when configuring the ACL, this command will display the rules of the ACL in the specified match order.

Examples

Display information about ACL 2000.

```
<Sysname> display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 1
```

Table 1-1 Description on the fields of the **display acl** command

Field	Description
Basic ACL 2000	The displayed information is about the basic ACL 2000.
1 rule	The ACL includes one rule.
Acl's step is 1	The step for rules of this ACL is 1.

display acl remaining entry

Syntax

display acl remaining entry

View

Any view

Parameter

None

Description

Use the **display acl remaning entry** command to display information about the remaining ACL resources.

According to the output, you can determine the number of resources consumed by a certain type of ACL rules and whether the exhaustion of resources causes the failure to assign ACL rules.

Example

Display information about the remaining ACL resources.

```
<Sysname> display acl remaining entry
  Resource  Total   Reserved  Configured  Remaining   Start     End
   Type      Number  Number    Number       Number    Port Name  Port Name
------------------------------------------------------------------------------
RULE/MASK    1024       64          1         959     GE1/0/1   GE1/0/24
  COUNTER      32        0          0          32     GE1/0/1   GE1/0/24
    METER     256        0          0         256     GE1/0/1   GE1/0/24
```

Table 1-2 Description on the fields of the **display acl remaining entry** command

Field	Description
Resource Type	Resource type, including: • RULE/MASK: number of rule resources that the switch can assign; • CONUTER: number of traffic statistics resources that the switch can assign; • METER: number of traffic limit resources that the switch can assign.
Total Number	Total number of ACL resources
Reserved Number	Number of resources reserved for system ACLs
Configured Number	Number of resources configured for user-defined ACLs
Remaining Number	Number of remaining resources
Start Port Name End Port Name	Start port number and end port number corresponding to the entry

display ipv6-acl-template

Syntax

display ipv6-acl-template

View

Any view

Parameter

None

Description

Use the **display ipv6-acl-template** command to display the IPv6 ACL template configuration information.

Example

Display the IPv6 ACL template configuration information.

```
<Sysname> display ipv6-acl-template
  Ipv6 acl template : src-ip dest-ip
```

display packet-filter

Syntax

display packet-filter { **global | interface** *interface-type interface-number* | **port-group** [*group-id*] | **unitid** *unit-id* **| vlan** [*vlan-id*] }

View

Any view

Parameter

global: Displays information about global packet filtering.

interface *interface-type interface-number*: Displays information about packet filtering on the port specified by *interface-type* and *interface-number*.

port-group *group-id*: Displays information about packet filtering on the port group specified by *group-id*.

unitid *unit-id*: Displays information about packet filtering on the unit specified by *unit-id*. The unit ID can be set only to 1.

vlan *vlan-id*: Displays information about packet filtering on the VLAN specified by *vlan-id*.

Description

Use the **display packet-filter** command to display information about packet filtering.

Example

Display information about packet filtering on the switch.

```
<Sysname> display packet-filter unitid 1
GigabitEthernet1/0/1
 Inbound:
 Acl 2000 rule 0  running
```

Table 1-3 Description on the fields of the **display packet-filter** command

Field	Description
GigabitEthernet1/0/1	Packet filtering is performed on GigabitEthernet1/0/1.
Inbound	Packet filtering is performed in the inbound direction.
Acl 2000 rule 0	The rule 0 of ACL 2000 is used.

Field	Description
running	Status of the rule, which can be • running: The ACL rule is active. • not running: The ACL rule is inactive. Usually, this is because the current time is out of the rule's time range.

display time-range

Syntax

display time-range { **all** | *time-name* }

View

Any view

Parameters

all: Displays all time ranges.

time-name: Name of a time range, a string of 1 to 32 characters that starts with a to z or A to Z.

Description

Use the **display time-range** command to display the configuration and status of a time range or all the time ranges. For active time ranges, this command displays "Active"; for inactive time ranges, this command displays "Inactive".

Related commands: **time-range**.

Examples

Display all time ranges.

```
<Sysname> display time-range all
Current time is 17:01:34 May/21/2007 Monday
Time-range : tr ( Active )
 12:00 to 18:00 working-day
Time-range : tr1 ( Inactive )
 From 12:00 Jan/1/2008 to 12:00 Jun/1/2008
```

Table 1-4 Description on the fields of the **display time-range** command.

Field	Description
Current time is 17:01:34 May/21/2007 Monday	Current system time
Time-range	Name of the time range
Active	Status of the time range, which can be: • Active: The time range is active currently. • Inactive: The time range is not inactive now.
12:00 to 18:00 working-day	The periodic time range is from 12:00 to 18:00 on each working day.

Field	Description
From 12:00 Jan/1/2008 to 12:00 Jun/1/2008	The absolute time range is from 12:00 January 1, 2008 to 12:00 June 1, 2008.

ipv6-acl-template

Syntax

ipv6-acl-template { **cos** | **dscp** | **dest-ip** | **dest-mac** | **dest-port** | **ip-protocol** | **icmpv6-type** | **icmpv6-code** | **src-ip** | **src-mac** | **src-port** | **vlan**} *

undo ipv6-acl-template

View

System view

Parameter

cos: Matches the cos field in IPv6 packets.

dscp: Matches the dscp field in IPv6 packets.

dest-ip: Matches the destination IP address field in IPv6 packets.

dest-mac: Matches the destination MAC address field in IPv6 packets.

dest-port: Matches the TCP/UDP destination port field in IPv6 packets.

ip-protocol: Matches the next header field in IPv6 packets.

icmpv6-type: Matches the ICMPv6 type field in IPv6 packets.

icmpv6-code: Matches the ICMPv6 code field in IPv6 packets.

src-ip: Matches the source IP address field in IPv6 packets.

src-mac: Matches the source MAC address field in IPv6 packets.

src-port: Matches the TCP/UDP source port field in IPv6 packets.

vlan: Matches the VLAN tag field in IPv6 packets.

Description

Use the **ipv6-acl-template** command to configure an IPv6 ACL template.

Use the **undo ipv6-acl-template** command to remove the configuration.

By default, no IPv6 ACL template is configured.

Note that:

- Only one IPv6 ACL template is supported on a 4200G switch.
- To specify the **src-port**, **dest-port**, **icmpv6-type** or **icmpv6-code** keyword in the command, you need to specify the **ip-protocol** keyword at first.
- If there is already a template, you need to remove it to configure a new one. If the template is referenced by an IPv6 ACL rule that has been applied, you cannot remove it.

Example

Configure an IPv6 ACL template to match the source address and destination address fields in IPv6 packets.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6-acl-template src-ip dest-ip
```

packet-filter

Syntax

packet-filter inbound *acl-rule*

undo packet-filter inbound *acl-rule*

View

System view, Ethernet port view, Port group view

Parameters

inbound: Filters inbound packets.

acl-rule: ACL/ACL rules to be applied. This argument can be one of those listed in Table 1-5.

Table 1-5 Combined application of ACLs

Combination mode	The *acl-rule* argument
Apply all the rules of an ACL that is of IP type (The ACL can be a basic ACL or an advanced ACL.)	**ip-group** *acl-number*
Apply a rule of an ACL that is of IP type (The ACL can be a basic ACL or an advanced ACL.)	**ip-group** *acl-number* **rule** *rule-id*
Apply all the rules of a Layer 2 ACL	**link-group** *acl-number*
Apply a rule of a Layer 2 ACL	**link-group** *acl-number* **rule** *rule-id*
Apply all rules of an IPv6 ACL	**user-group** *acl-number*
Apply a rule of an IPv6 ACL	**user-group** *acl-number* **rule** *rule-id*
Apply a rule of an ACL that is of IP type and a rule of a Layer 2 ACL	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

In Table 1-5:

- The **ip-group** *acl-number* keyword specifies a basic or an advanced ACL. The *acl-number* argument ranges from 2000 to 3999.
- The **link-group** *acl-number* keyword specifies a Layer 2 ACL. The *acl-number* argument ranges from 4000 to 4999.
- The **user-group** *acl-number* keyword specifies an IPv6 ACL. The *acl-number* argument ranges from 5000 to 5999.
- The **rule** *rule-id* keyword specifies a rule of an ACL. The *rule* argument ranges from 0 to 65534. If you do not specify this argument, all the rules of the ACL are applied.

Description

Use the **packet-filter** command to assign an ACL globally, to a port, or in a port group to filter inbound packets.

Use the **undo packet-filter** command to cancel the assignment of an ACL.

Examples

Apply all rules of basic ACL 2000 on GigabitEthernet 1/0/1 to filter inbound packets. Here, it is assumed that the ACL and its rules are already configured.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter inbound ip-group 2000
[Sysname-GigabitEthernet1/0/1] quit
```

Apply rule 1 of advanced ACL 3000 and rule 2 of Layer 2 ACL 4000 on GigabitEthernet 1/0/4 to filter inbound packets. Here, it is assumed that the ACLs and their rules are already configured.

```
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] packet-filter inbound ip-group 3000 rule 1 link-group 4000 rule 2
```

After completing the above configuration, you can use the **display packet-filter** command to view information about packet filtering.

packet-filter vlan

Syntax

packet-filter vlan *vlan-id* **inbound** *acl-rule*

undo packet-filter vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

vlan-id: VLAN ID.

inbound: Specifies to filter packets received by the ports in the VLAN.

acl-rule: ACL rules to be applied, which can be a combination of the rules of multiple ACLs, as described in Table 1-5.

Description

Use the **packet-filter vlan** command to apply ACL rules to a VLAN to filter packets.

Use the **undo packet-filter vlan** command to remove the application of ACL rules to a VLAN.

When you need to apply an ACL to all ports in a VLAN, you can use the **packet-filter vlan** command to achieve the goal in one operation.

Note

An ACL assigned to a VLAN takes effect only for the packets tagged with 802.1Q header. For more information about 802.1Q header, refer to the VLAN part.

Examples

Apply all rules of basic ACL 2000 to VLAN 10 to make all ports in VLAN 10 filter inbound packets. Here, it is assumed that the ACL and its rules and the VLAN are already configured.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] packet-filter vlan 10 inbound ip-group 2000
```

After completing the above configuration, you can use the **display packet-filter** command to view information about packet filtering.

rule (for Basic ACLs)

Syntax

rule [*rule-id*] { **deny** | **permit**} [*rule-string*]

undo rule *rule-id* [**fragment** | **source** | **time-range**]*

View

Basic ACL view

Parameters

Parameters of the rule command

rule-id: ACL rule ID, in the range of 0 to 65534.

deny: Drops the matched packets.

permit: Permits the matched packets.

rule-string: ACL rule information, which can be a combination of the parameters described in Table 1-6.

Table 1-6 Parameters for basic IPv4 ACL rules

Parameters	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address.	The *sour-addr sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.
fragment	Indicates that the rule applies only to non-tail fragments.	—
time-range *time-name*	Specifies the time range in which the rule takes effect.	*time-name*: specifies the name of the time range in which the rule is active; a string comprising 1 to 32 characters.

Note

sour-wildcard is the complement of the wildcard mask of the source subnet mask. For example, you need to input 0.0.255.255 to specify the subnet mask 255.255.0.0.

Parameters of the undo rule command

rule-id: Rule ID, which must the ID of an existing ACL rule. You can obtain the ID of an ACL rule by using the **display acl** command.

fragment: Removes the settings concerning non-tail fragments in the ACL rule.

source: Removes the settings concerning source address in the ACL rule.

time-range: Removes the settings concerning time range in the ACL rule.

Description

Use the **rule** command to define an ACL rule.

Use the **undo rule** command to remove an ACL rule or specified settings of an ACL rule.

To remove an ACL rule using the **undo rule** command, you need to provide the ID of the ACL rule. If no other arguments are specified, the entire ACL rule is removed. Otherwise, only the specified information of the ACL rule is removed.

Note that:

- With the **config** match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- With the **auto** match order specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Examples

Create basic ACL 2000 and define rule 1 to deny packets whose source IP addresses are 192.168.0.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 deny source 192.168.0.1 0
[Sysname-acl-basic-2000] quit
```

Create basic ACL 2001 and define rule 1 to deny packets that are non-tail fragments.

```
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 1 deny fragment
[Sysname-acl-basic-2001] quit
```

Create basic ACL 2002 and define rule 1 to deny all packets during the period specified by time range trname.

```
[Sysname] acl number 2002
[Sysname-acl-basic-2002] rule 1 deny time-range trname
```

After completing the above configuration, you can use the **display acl** command to view the configuration information of the ACLs.

rule (for Advanced ACLs)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [*rule-string*]

undo rule *rule-id* [**destination** | **destination-port** | **dscp** | **fragment** | **icmp-type** | **precedence** | **source** | **source-port** | **time-range** | **tos**]*

View

Advanced ACL view

Parameters

Parameters of the rule command

rule-id: ACL rule ID, in the range of 0 to 65534.

deny: Drops the matched packets.

permit: Permits the matched packets.

protocol: Protocol carried by IP. When the protocol is represented by numeral, it ranges from 1 to 255; when the protocol is represented by name, it can be **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), and **udp** (17).

rule-string: ACL rule information, which can be a combination of the parameters described in Table 1-7.

Table 1-7 Arguments/keywords available to the *rule-string* argument

Arguments/Keywords	Type	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Source address	Specifies the source address information for the ACL rule	The *sour-addr sour-wildcard* arguments specify the source address of the packets, expressed in dotted decimal notation. You can specify the IP address of a host as the source address by providing 0 for the *sour-wildcard* argument. The **any** keyword specifies any source address.

Arguments/Keywords	Type	Function	Description
destination { *dest-addr dest-wildcard* | **any** }	Destination address	Specifies the destination address information for the ACL rule	The *dest-addr dest-wildcard* arguments specify the destination address of the packets, expressed in dotted decimal notation. You can specify the IP address of a host as the destination address by providing 0 for the *dest-wildcard* argument. The **any** keyword specifies any destination address.
precedence *precedence*	Packet priority	Specifies an IP precedence.	The *precedence* argument can be a number in the range 0 to 7.
tos *tos*	Packet priority	Specifies a ToS preference.	The *tos* argument can be a number in the range 0 to 15.
dscp *dscp*	Packet priority	Specifies a DSCP priority.	The *dscp* argument can be a number in the range 0 to 63.
fragment	Fragment information	Indicates that the rule applies only to non-tail fragments.	—
time-range *time-name*	Time range information	Specifies the time range in which the rule takes effect.	*time-name*: specifies the name of the time range in which the rule is active; a string comprising 1 to 32 characters.

Note

The *sour-wildcard*/*dest-wildcard* argument is the complement of the wildcard mask of the source/destination subnet mask. For example, you need to input 0.0.255.255 to specify the subnet mask 255.255.0.0.

If you specify the **dscp** keyword, you can directly input a value ranging from 0 to 63 or input one of the keywords listed in Table 1-8 as DSCP.

Table 1-8 DSCP values and the corresponding keywords

Keyword	DSCP value in decimal	DSCP value in binary
af11	10	001010

Keyword	DSCP value in decimal	DSCP value in binary
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
be	0	000000
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
ef	46	101110

If you specify the **precedence** keyword, you can directly input a value ranging from 0 to 7 or input one of the keywords listed in Table 1-9 as IP precedence.

Table 1-9 IP Precedence values and the corresponding keywords

Keyword	IP Precedence in decimal	IP Precedence in binary
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

If you specify the **tos** keyword, you can directly input a value ranging from 0 to 15 or input one of the keywords listed in Table 1-10 as the ToS value.

Table 1-10 ToS value and the corresponding keywords

Keyword	ToS in decimal	ToS in binary
normal	0	0000
min-monetary-cost	1	0001
max-reliability	2	0010
max-throughput	4	0100
min-delay	8	1000

If the protocol type is TCP or UDP, you can also define the information listed in Table 1-11.

Table 1-11 TCP/UDP-specific ACL rule information

Parameters	Type	Function	Description
source-port *operator port1* [*port2*]	Source port	Defines the source port information of UDP/TCP packets	The value of *operator* can be **lt** (less than), **gt** (greater than), **eq** (equal to), **neq** (not equal to) or **range** (within the range of). Only the **range** operator requires two port numbers as the operands. The other operators require only one port number as the operand. *port1* and *port2*: TCP/UDP port number(s), expressed as port names or port numbers. When expressed as numerals, the value range is 0 to 65535.
destination-port *operator port1* [*port2*]	Destination port	Defines the destination port information of UDP/TCP packets	
established	TCP connection flag	Specifies that the rule is applicable only to the first SYN segment for establishing a TCP connection	TCP-specific argument

If TCP or UDP port number is represented by name, you can also define the information listed in Table 1-12.

Table 1-12 TCP or UDP port values

Type	Value
TCP	**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), **www** (80)
UDP	**biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177)

Note

Note the following when assigning an advanced ACL to the hardware on Switch 4200G series:

- The precedence and tos keywords are not supported.
- When defining ACL rules for TCP/UDP packets, operator (in Table 1-11) can only be "**eq**".

If the protocol type is ICMP, you can also define the information listed in Table 1-13.

Table 1-13 ICMP-specific ACL rule information

Parameters	Type	Function	Description
icmp-type *icmp-type icmp-code*	Type and message code information of ICMP packets	Specifies the type and message code information of ICMP packets in the ACL rule	*icmp-type*: ICMP message type, ranging from 0 to 255 *icmp-code*: ICMP message code, ranging from 0 to 255

If the protocol type is ICMP, you can also just input the ICMP message name after the **icmp-type** keyword. See Table 1-14 for ICMP messages.

Table 1-14 ICMP messages

Name	ICMP type	ICMP code
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0

Name	ICMP type	ICMP code
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=0

Parameters of the undo rule command

rule-id: Rule ID, which must the ID of an existing ACL rule. You can obtain the ID of an ACL rule by using the **display acl** command.

source: Removes the settings concerning the source address in the ACL rule.

source-port: Removes the settings concerning the source port in the ACL rule. This keyword is only available to the ACL rules with their protocol types set to TCP or UDP.

destination: Removes the settings concerning the destination address in the ACL rule.

destination-port: Removes the settings concerning the destination port in the ACL rule. This keyword is only available to the ACL rules with their protocol types set to TCP or UDP.

icmp-type: Removes the settings concerning the ICMP type and message code in the ACL rule. This keyword is only available to the ACL rules with their protocol type set to ICMP.

precedence: Removes the precedence-related settings in the ACL rule.

tos: Removes the ToS-related settings in the ACL rule.

dscp: Removes the DSCP-related settings in the ACL rule.

time-range: Removes the time range settings in the ACL rule.

fragment: Removes the settings concerning non-tail fragments in the ACL rule.

Description

Use the **rule** command to define an ACL rule.

Use the **undo rule** command to remove an ACL rule or specified settings of an ACL rule.

To remove an ACL rule using the **undo rule** command, you need to provide the ID of the ACL rule. If no other arguments are specified, the entire ACL rule is removed. Otherwise, only the specified information of the ACL rule is removed.

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- If the ACL is created with the **auto** keyword specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Examples

Create advanced ACL 3000 and define rule 1 to deny packets with the source IP address of 192.168.0.1 and DSCP priority of 46.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 1 deny ip source 192.168.0.1 0 dscp 46
[Sysname-acl-adv-3000] quit
```

Create advanced ACL 3001 and define rule 1 to permit TCP packets that are sourced from network 129.9.0.0/16, destined for network 202.38.160.0/24, and using the destination port number of 80.

```
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule 1 permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80
```

After completing the above configuration, you can use the **display acl** command to view the configuration information of the ACLs.

rule (for Layer 2 ACLs)

Syntax

rule [*rule-id*] { **deny** | **permit** } [*rule-string*]

undo rule *rule-id*

View

Layer 2 ACL view

Parameters

rule-id: ACL rule ID, in the range of 0 to 65534.

deny: Drops the matched packets.

permit: Permits the matched packets.

rule-string: ACL rule information, which can be a combination of the arguments/keywords described in Table 1-15.

Table 1-15 Layer 2 ACL rule information

Parameters	Type	Function	Description
format-type	Link layer encapsulation type	Specifies the link layer encapsulation type in the rule	This argument can be 802.3/802.2, 802.3, ether_ii, or snap.
lsap *lsap-code lsap-wildcard*	lsap field	Specifies the lsap field for the ACL rule	*lsap-code*: Encapsulation format of data frames, a 16-bit hexadecimal number. *lsap-wildcard*: Mask of the lsap value, a 16-bit hexadecimal number used to specify the mask bits.

Parameters	Type	Function	Description
source { *source-mac-addr source-mac-mask* | *vlan-id* }*	Source MAC address information or source VLAN information	Specifies the source MAC address range or source VLAN range for the ACL rule	*source-mac-addr*: Source MAC address, in the format of H-H-H. *source-mac-mask*: Mask of the source MAC address, in the format of H-H-H. *vlan-id*: Source VLAN ID, in the range of 1 to 4,094.
dest *dest-mac-addr dest-mac-mask*	Destination MAC address information	Specifies the destination MAC address range for the ACL rule	*dest-mac-addr*: Destination MAC address, in the format of H-H-H. *dest-mac-mask*: Mask of the destination MAC address, in the format of H-H-H.
cos *cos*	Priority	Specifies the 802.1p priority of the rule	*cos*: VLAN priority, in the range of 0 to 7.
time-range *time-name*	Time range information	Specifies the time range in which the rule takes effect.	*time-name*: specifies the name of the time range in which the rule is active; a string comprising 1 to 32 characters.
type *protocol-type protocol-mask*	Protocol type of Ethernet frames	Specifies the protocol type of Ethernet frames for the ACL rule	*protocol-type*: Protocol type. *protocol-mask*: Protocol type mask.

Note

As for Layer 2 ACLs to be assigned to the hardware, Switch 4200G series do not support ACL rules with the *format-type* argument or the **lsap** *keyword* specified.

Description

Use the **rule** command to define an ACL rule.

Use the **undo rule** command to remove an ACL rule.

To remove an ACL rule using the **undo rule** command, you need to provide the ID of the ACL rule. You can obtain the ID of an ACL rule by using the **display acl** command.

Note that:

- You can modify any existent rule of the Layer 2 ACL and the unmodified part of the ACL remains.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.

- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

Examples

Create Layer 2 ACL 4000 and define rule 1 to deny packets that are sourced from MAC address 000d-88f5-97ed, destined for MAC address 0011-4301-991e, and using the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 1 deny cos 3 source 000d-88f5-97ed ffff-ffff-ffff dest
0011-4301-991e ffff-ffff-ffff
[Sysname-acl-ethernetframe-4000] quit
```

After completing the above configuration, you can use the **display acl** command to view the configuration information of the ACLs.

rule (for IPv6 ACLs)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**src-mac** *rule-string rule-mask*] [**dest-mac** *rule-string rule-mask*] [**cos** *rule-string rule-mask*] [**dscp** *rule-string rule-mask*] [**vlan** *rule-string rule-mask*] [**ip-protocol** *rule-string rule-mask*] [**src-ip** *ipv6-address prefix-length*] [**dest-ip** *ipv6-address prefix-length*] [[**src-port** *rule-string rule-mask* | **dest-port** *rule-string rule-mask*] ***** | [**icmpv6-type** *rule-string rule-mask* | **icmpv6-code** *rule-string rule-mask*] *****] [**time-range** *time-name*]

undo rule *rule-id*

View

IPv6 ACL view

Parameter

rule-id: ACL rule ID, in the range of 0 to 65534.

deny: Drops the matched packets.

permit: Permits the matched packets.

src-mac *rule-string rule-mask*: Specifies the source IPv6 MAC address information. Arguments *rule-string* and *rule-mask* indicate the IPv6 source MAC address and mask and consist of twelve hexadecimal numbers respectively.

dest-mac *rule-string rule-mask*: Specifies the destination IPv6 MAC address information. Arguments *rule-string* and *rule-mask* indicate the IPv6 destination MAC address and mask and consist of twelve hexadecimal numbers respectively.

cos *rule-string rule-mask*: Specifies the CoS information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of two hexadecimal numbers respectively.

dscp *rule-string rule-mask*: Specifies the traffic class information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of two hexadecimal numbers respectively.

vlan *rule-string rule-mask*: Specifies the IPv6 VLAN tag information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of four hexadecimal numbers respectively.

ip-protocol *rule-string rule-mask*: Specifies the next header information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of two hexadecimal numbers respectively.

src-ip *ipv6-address prefix-length*: Specifies the source IPv6 address information. Arguments *ipv6-address* and *prefix-length* indicate the IPv6 address and prefix length respectively, where *prefix-length* must be in the range 1 to 128.

dest-ip *ipv6-address prefix-length*: Specifies the destination IPv6 address information. Arguments *ipv6-address* and *prefix-length* indicate the IPv6 address and prefix length respectively, where *prefix-length* must be in the range 1 to 128.

src-port *rule-string rule-mask*: Specifies the source TCP/UDP port information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of four hexadecimal numbers respectively.

dest-port *rule-string rule-mask*: Specifies the destination TCP/UDP port information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of four hexadecimal numbers respectively.

icmpv6-type *rule-string rule-mask*: Specifies the ICMPv6 type information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of two hexadecimal numbers respectively.

icmpv6-code *rule-string rule-mask*: Specifies the ICMPv6 code information. Arguments *rule-string* and *rule-mask* indicate the content string and mask and consist of two hexadecimal numbers respectively.

time-range *time-name*: Specifies the time range in which the rule takes effect. *time-name* indicates the name of a time range and must be a case-insensitive string of 1 to 32 characters that starts with an English letter. To avoid confusion, it cannot be **all**.

Description

Use the **rule** command to define an ACL rule.

Use the **undo rule** command to remove an ACL rule.

To remove an ACL rule, you need to specify the number of the ACL rule. You can use the **display acl** command to view the number of an ACL rule.

Note that:

- You can modify any existent rule of an IPv6 ACL. If you modify only the action to be taken or the time range, the unmodified part of the rule remains the same. If you modify the contents of a user-defined string, the new string overwrites the original one.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule of the ACL; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- To specify the **src-port** or **dest-port** keyword for a rule, you need to specify the **ip-protocol** *rule-string rule-mask* combination as TCP or UDP, that is, 0x06 or 0x11. To specify the **icmpv6-type** or **icmpv6-code** keyword for a rule, you need to specify the **ip-protocol** *rule-string rule-mask* combination as ICMPv6, that is, 0x3a.

🕮 **Note:**

Note the following when assigning an IPv6 ACL to the hardware on Switch 4200G Series:

- IPv6 ACLs do not match IPv6 packets with extension headers.
- Do not use IPv6 ACLs with VLAN mapping and trusted port priority.

Example

Configure an rule for IPv6 ACL 5000, denying packets from 3001::1/64 to 3002::1/64.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule deny src-ip 3001::1 64 dest-ip 3002::1 64
```

rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View

Advanced ACL view, Layer 2 ACL view, IPv6 ACL view

Parameters

rule-id: ID of the ACL rule, in the range of 0 to 65534.

text: Comment for the ACL rule, a string of 1 to 127 characters. Blank spaces and special characters are acceptable.

Description

Use the **rule comment** command to define a comment for the ACL rule.

Use the **undo rule comment** command to remove the comment defined for the ACL rule.

You can give rules comments to provide relevant information such as their application purposes and the ports they are applied to, so that you can easily identity and distinguish ACL rules by their comments.

By default, an ACL rule has no comment.

Before defining a comment for an ACL rule, make sure that the ACL rule exists.

Examples

Define the comment “This rule is to be applied to GigabitEthernet 1/0/1” for rule 0 of advanced ACL 3001.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule 0 comment This rule is to be applied to GigabitEthernet 1/0/1
```

Use the **display acl** command to view the configuration information of advanced ACL 3001.

```
[Sysname-acl-adv-3001] display acl 3001
Advanced ACL  3001, 1 rule
```

```
Acl's step is 1
 rule 0 deny IP source 1.1.1.1 0 destination 2.2.2.2 0
 rule 0 comment This rule is to be applied to GigabitEthernet 1/0/1
```

time-range

Syntax

time-range *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }

undo time-range { **all** | **name** *time-name* [*start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date*] }

View

System view

Parameters

all: Removes all the time ranges.

time-name: Name of a time range, a case insensitive string of 1 to 32 characters that starts with a to z or A to Z. To avoid confusion, it cannot be all.

start-time: Start time of a periodic time range, in the form of hh:mm.

end-time: End time of a periodic time range, in the form of hh:mm. The end time must be greater than the start time.

days-of-the-week: Day of the week when the periodic time range is active. You can provide this argument in one of the following forms.

- Numeral (0 to 6)
- Mon, Tue, Wed, Thu, Fri, Sat, and Sun
- Working days (Monday through Friday)
- Off days (Saturday and Sunday)
- Daily, namely everyday of the week

from *start-time start-date*: Specifies the start date of an absolute time range, in the form of hh:mm MM/DD/YYYY or hh:mm YYYY/MM/DD. The *start-time start-date* and *end-time end-date* argument jointly define a period in which the absolute time range takes effect. If the start date is not specified, the time range starts from 1970/01/01 00:00.

to *end-time end-date*: Specifies the end date of an absolute time range, in the form of hh:mm MM/DD/YYYY or hh:mm YYYY/MM/DD. The *start-time start-date* and *end-time end-date* argument jointly define a period in which the absolute time range takes effect. If the end date is not specified, the time range ends at 2100/12/31 23:59.

Description

Use the **time-range** command to define a time range.

Use the **undo time-range** command to remove the specified or all time ranges.

Note that:

- If only a periodic time section is defined in a time range, the time range is active only when the system time is within the defined periodic time section. If multiple periodic time sections are defined

in a time range, the time range is active only when the system time is within one of the periodic time sections.

- If only an absolute time section is defined in a time range, the time range is active only when the system time is within the defined absolute time section. If multiple absolute time sections are defined in a time range, the time range is active only when the system time is within one of the absolute time sections.
- If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range defines an absolute time section from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section from 12:00 to 14:00 every Wednesday. This time range is active only when the system time is within 12:00 to 14:00 every Wednesday in 2004.

Examples

Define a periodic time range that is active from 08:00 to 12:00 every working day.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] time-range tr1 08:00 to 12:00 working-day
```

Define an absolute time range that is active from 12:00 January 1, 2008 to 12:00 June 1, 2008.

```
[Sysname] time-range tr2 from 12:00 1/1/2008 to 12:00 6/1/2008
```

Display the configuration information of the time ranges.

```
[Sysname] display time-range all
Current time is 17:37:23 Nov/27/2007 Tuesday

Time-range : tr1 ( Inactive )
 08:00 to 12:00 working-day

Time-range : tr2 ( Inactive )
 From 12:00 Jan/1/2008 to 12:00 Jun/1/2008
```

Table of Contents

1 QoS Commands

QoS Commands

burst-mode enable

Syntax

burst-mode enable

undo burst-mode enable

View

System view

Parameters

None

Description

Use the **burst-mode enable command** to enable the burst function.

Use the **undo burst-mode enable** command to disable the burst function.

By default, the burst function is disabled.

The burst function improves packet buffering and forwarding performance in the following scenarios:

- Dense broadcast or multicast traffic and massive burst traffic are present.
- High-speed traffic is forwarded over a low-speed link or traffic received from multiple interfaces at the same speed is forwarded through an interface at the same speed.

By enabling the burst function on your device, you can improve the processing performance of the device operating in the above scenarios and thus reduce packet loss rate.

Note

Because the burst function may affect the QoS performance of your device, you must make sure that you are fully aware of the impacts when enabling the burst function.

Examples

Enable the burst function on a Switch 4200G.

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

display protocol-priority

Syntax

display protocol-priority

View

Any view

Parameters

None

Description

Use the **display protocol-priority** command to display the list of protocol priorities you assigned with the **protocol-priority** command.

A Switch 4200G supports setting priorities for certain protocol packets generated by it. The supported protocols are Telnet, SNMP, and ICMP. Depending on your configuration, the IP or DSCP value is displayed for a specified protocol.

Related commands: **protocol-priority**.

Examples

Display the list of protocol priorities manually specified.

```
<Sysname> display protocol-priority
Protocol: telnet
  DSCP: be(0)
```

display qos cos-drop-precedence-map

Syntax

display qos cos-drop-precedence-map

View

Any view

Parameters

None

Description

Use the **display qos cos-drop-precedence-map** command to display the CoS-precedence-to-drop-precedence mapping table. Note that the CoS precedence is also referred to as the 802.1p precedence in this document.

Related commands: **qos cos-drop-precedence-map**.

Examples

Display the CoS-precedence-to-drop-precedence mapping table on a Switch 4200G.

```
<Sysname> display qos cos-drop-precedence-map
cos-drop-precedence-map:
```

```
              cos :       0     1     2     3     4     5     6     7
 ------------------------------------------------------------------------
  drop-precedence :       0     0     0     0     0     0     0     0
```

display qos cos-dscp-map

Syntax

display qos cos-dscp-map

View

Any view

Parameters

None

Description

Use the **display qos cos-dscp-map** command to display the CoS-precedence-to-DSCP mapping table.

Related commands: **qos cos-dscp-map**.

Examples

Display the CoS-precedence-to-DSCP mapping table.

```
<Sysname> display qos cos-dscp-map
cos-dscp-map:
              cos :      0     1     2     3     4     5     6     7
 ------------------------------------------------------------------------
             dscp :     16     0     8    24    32    40    48    56
```

display qos cos-local-precedence-map

Syntax

display qos cos-local-precedence-map

View

Any view

Parameters

None

Description

Use the **display qos cos-local-precedence-map** command to display the CoS-precedence-to-local-precedence mapping table.

Related commands: **qos cos-local-precedence-map**.

Examples

Display the CoS-precedence-to-local-precedence mapping table on a Switch 4200G.

```
<Sysname> display qos cos-local-precedence-map
```

```
 cos-local-precedence-map:
              cos(802.1p) :      0      1      2      3      4      5      6      7
-------------------------------------------------------------------------------
   local precedence(queue) :     2     0     1     3     4     5     6     7
```

display qos dscp-cos-map

Syntax

display qos dscp-cos-map

View

Any view

Parameters

None

Description

Use the **display qos dscp-cos-map** command to display the DSCP-to-CoS-precedence mapping table.

Related commands: **qos dscp-cos-map**.

Examples

Display the DSCP-to-CoS-precedence mapping table.

```
<Sysname> display qos dscp-cos-map
 dscp-cos-map:
             dscp :          cos
 ---------------------------------------------
               0 :            1
               1 :            1
               2 :            1
               3 :            1
               4 :            1
               5 :            1
               6 :            1
               7 :            1
               8 :            2
               9 :            2
              10 :            2
              11 :            2
              12 :            2
              13 :            2
              14 :            2
              15 :            2
              16 :            0
              17 :            0
              18 :            0
              19 :            0
```

```
20 :            0
21 :            0
22 :            0
23 :            0
24 :            3
25 :            3
26 :            3
27 :            3
28 :            3
29 :            3
30 :            3
31 :            3
32 :            4
33 :            4
34 :            4
35 :            4
36 :            4
37 :            4
38 :            4
39 :            4
40 :            5
41 :            5
42 :            5
43 :            5
44 :            5
45 :            5
46 :            5
47 :            5
48 :            6
49 :            6
50 :            6
51 :            6
52 :            6
53 :            6
54 :            6
55 :            6
56 :            7
57 :            7
58 :            7
59 :            7
60 :            7
61 :            7
62 :            7
63 :            7
```

display qos dscp-drop-precedence-map

Syntax

display qos dscp-drop-precedence-map

View

Any view

Parameters

None

Description

Use the **display qos dscp-drop-precedence-map** command to display the DSCP-to-drop-precedence mapping table.

Related commands: **qos dscp-drop-precedence-map**.

Examples

Display the DSCP-to-drop-precedence mapping table on a Switch 4200G.

```
<Sysname> display qos dscp-drop-precedence-map
 dscp-drop-precedence-map:
             dscp : drop-precedence
 ----------------------------------------------
                0 :            1
                1 :            1
                2 :            1
                3 :            1
                4 :            1
                5 :            1
                6 :            1
                7 :            1
                8 :            1
                9 :            1
               10 :            1
               11 :            1
               12 :            1
               13 :            1
               14 :            1
               15 :            1
               16 :            1
               17 :            1
               18 :            1
               19 :            1
               20 :            1
               21 :            1
               22 :            1
               23 :            1
               24 :            1
```

```
25 :            1
26 :            1
27 :            1
28 :            1
29 :            1
30 :            1
31 :            1
32 :            0
33 :            0
34 :            0
35 :            0
36 :            0
37 :            0
38 :            0
39 :            0
40 :            0
41 :            0
42 :            0
43 :            0
44 :            0
45 :            0
46 :            0
47 :            0
48 :            0
49 :            0
50 :            0
51 :            0
52 :            0
53 :            0
54 :            0
55 :            0
56 :            0
57 :            0
58 :            0
59 :            0
60 :            0
61 :            0
62 :            0
63 :            0
```

display qos dscp-dscp-map

Syntax

display qos dscp-dscp-map

View

Any view

Parameters

None

Description

Use the **display qos dscp-dscp-map** command to display the DSCP-to-DSCP mapping table.

Related commands: **qos dscp-dscp-map**.

Examples

Display the DSCP-to-DSCP mapping table.

```
<Sysname> display qos dscp-dscp-map
 dscp-dscp-map:
             dscp :         dscp
 ---------------------------------------------
                0 :            0
                1 :            1
                2 :            2
                3 :            3
                4 :            4
                5 :            5
                6 :            6
                7 :            7
                8 :            8
                9 :            9
               10 :           10
               11 :           11
               12 :           12
               13 :           13
               14 :           14
               15 :           15
               16 :           16
               17 :           17
               18 :           18
               19 :           19
               20 :           20
               21 :           21
               22 :           22
               23 :           23
               24 :           24
               25 :           25
               26 :           26
               27 :           27
               28 :           28
               29 :           29
               30 :           30
               31 :           31
               32 :           32
               33 :           33
```

```
34 :            34
35 :            35
36 :            36
37 :            37
38 :            38
39 :            39
40 :            40
41 :            41
42 :            42
43 :            43
44 :            44
45 :            45
46 :            46
47 :            47
48 :            48
49 :            49
50 :            50
51 :            51
52 :            52
53 :            53
54 :            54
55 :            55
56 :            56
57 :            57
58 :            58
59 :            59
60 :            60
61 :            61
62 :            62
63 :            63
```

display qos dscp-local-precedence-map

Syntax

display qos dscp-local-precedence-map

View

Any view

Parameters

None

Description

Use the **display qos dscp-local-precedence-map** command to display the DSCP-to-local-precedence mapping table.

Related commands: **qos dscp-local-precedence-map**.

Examples

Display the DSCP-to-local-precedence mapping table on a Switch 4200G.

```
<Sysname> display qos dscp-local-precedence-map
 dscp-local-precedence-map:
             dscp : local-precedence(queue)
 ------------------------------------------------
                0 :            0
                1 :            0
                2 :            0
                3 :            0
                4 :            0
                5 :            0
                6 :            0
                7 :            0
                8 :            1
                9 :            1
               10 :            1
               11 :            1
               12 :            1
               13 :            1
               14 :            1
               15 :            1
               16 :            2
               17 :            2
               18 :            2
               19 :            2
               20 :            2
               21 :            2
               22 :            2
               23 :            2
               24 :            3
               25 :            3
               26 :            3
               27 :            3
               28 :            3
               29 :            3
               30 :            3
               31 :            3
               32 :            4
               33 :            4
               34 :            4
               35 :            4
               36 :            4
               37 :            4
               38 :            4
               39 :            4
               40 :            5
```

```
41 :            5
42 :            5
43 :            5
44 :            5
45 :            5
46 :            5
47 :            5
48 :            6
49 :            6
50 :            6
51 :            6
52 :            6
53 :            6
54 :            6
55 :            6
56 :            7
57 :            7
58 :            7
59 :            7
60 :            7
61 :            7
62 :            7
63 :            7
```

display qos-global

Syntax

display qos-global { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }

View

Any view

Parameters

all: Displays all the global QoS configurations.

traffic-limit: Displays the global traffic policing configuration and the traffic policing statistics.

traffic-priority: Displays the global priority marking configuration.

traffic-redirect: Displays the global traffic redirecting configuration.

traffic-statistics: Displays the global traffic accounting configuration and the collected traffic statistics.

Description

Use the **display qos-global** command to display the specific global QoS configuration or all the global QoS configurations.

Related commands: **mirrored-to**, **traffic-limit**, **traffic-priority**, **traffic-redirect**, **traffic-statistic**.

Examples

Display all the global QoS configurations.

```
<Sysname> display qos-global all
 global: traffic-limit inbound:
   Matches: Acl 3001 rule 0  running
     Target rate: 128 Kbps
     Exceed action: drop
   meter-statistic not running
```

Table 1-1 display qos-global all command output description

Field	Description
Global	QoS features configured globally, including: • traffic-limit: Traffic policing configuration. For description on fields related to this feature, refer to Table 1-5. • traffic-priority: Priority marking configuration. For description on fields related to this feature, refer to Table 1-6. • traffic-redirect: Traffic redirecting configuration. For description on fields related to this feature, refer to Table 1-7. • traffic-statistic: Traffic accounting configuration. For description on fields related to this feature, refer to Table 1-10. • mirrored-to: Traffic mirroring configuration. For description on fields related to this feature, refer to Table 1-3.

display qos-interface all

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **all**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, for which all the QoS configurations is to be displayed.

unit-id: Unit ID of a switch, for which all the configurations are to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface all** command to display all the QoS configurations of a port or a unit.

For Switch 4200G series, the following information is displayed in the following order depending on the configuration:

- Traffic policing configurations
- Priority marking configurations
- Traffic redirecting configurations
- Traffic accounting configurations
- Traffic mirroring configurations
- Priority trust mode configurations

- Traffic shaping configurations
- VLAN mapping configurations

Related commands: **line-rate**, **mirrored-to**, **priority-trust**, **traffic-limit**, **traffic-priority**, **traffic-redirect**, **traffic-remark-vlanid**, **traffic-shape**, **traffic-statistic**.

Examples

Display all the QoS configurations of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 all

GigabitEthernet1/0/1: traffic-limit
 Inbound:
   Matches: Acl 2000 rule 0  running
     Target rate: 128 Kbps
   meter-statistic not running

 GigabitEthernet1/0/1: priority-trust port

 GigabitEthernet1/0/1 Port Shaping: Disable
 0 kbps, 0 burst
 QID:    status    max-rate(kbps)   burst-size(byte)
-----------------------------------------------------
  0 :    Enable         640                16
  1 :   Disable           0                 0
  2 :   Disable           0                 0
  3 :   Disable           0                 0
  4 :   Disable           0                 0
  5 :   Disable           0                 0
  6 :   Disable           0                 0
  7 :   Disable           0                 0
```

Table 1-2 display qos-interface all command output description

Field	Description
GigabitEthernet1/0/1	QoS features configured on the port, including: • traffic-limit: Traffic policing configuration. For description on fields related to this feature, refer to Table 1-5. • traffic-priority: Priority marking configuration. For description on fields related to this feature, refer to Table 1-6. • traffic-redirect: Traffic redirecting configuration. For description on fields related to this feature, refer to Table 1-7. • traffic-statistic: Traffic accounting configuration. For description on fields related to this feature, refer to Table 1-10. • mirrored-to: Traffic mirroring configuration. For description on fields related to this feature, refer to Table 1-3. • priority-trust: Priority trust mode configuration. For description on fields related to this feature, refer to Table 1-4. • Port Shaping: Traffic shaping configuration. For description on fields related to this feature, refer to Table 1-9. • traffic-remark-vlanid: VLAN mapping configuration. For description on fields related to this feature, refer to Table 1-8.

display qos-interface mirrored-to

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **mirrored-to**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose traffic mirroring configuration is to be displayed.

unit-id: Unit ID of a switch, whose traffic mirroring configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface mirrored-to** command to display the traffic mirroring configuration of a port or all the ports on the device.

Related commands: **mirrored-to**.

Examples

Display the traffic mirroring configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 mirrored-to
GigabitEthernet1/0/1: mirrored-to
 Inbound:
   Matches: Acl 2000 rule 0  running
     Mirrored to: monitor interface
```

Table 1-3 display qos-interface mirrored-to command output description

Field	Description
GigabitEthernet1/0/1:	Port with traffic mirroring configured.
Inbound	Traffic mirroring is performed for incoming packets.
Matches	Match criteria.
Mirrored to	Mirror packets to the monitor port.

display qos-interface priority-trust

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **priority-trust**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose priority trust mode configuration is to be displayed.

unit-id: Unit ID of a switch, whose priority trust mode configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface priority-trust** command to display the priority trust mode configuration of a port or all the ports on the device.

Related commands: **priority-trust**.

Examples

Display the priority trust mode configuration of Gigabitethernet 1/0/1.

```
<Sysname> display qos-interface Gigabitethernet 1/0/1 priority-trust

 GigabitEthernet1/0/1: priority-trust port
```

Table 1-4 display qos-interface priority-trust command output description

Field	Description
GigabitEthernet1/0/1	The priority trust mode configured on the port, which can be: • **priority-trust port**: Indicates that port priority is trusted • **priority-trust cos**: Indicates that the 802.1p precedence values of received packets are trusted • **priority-trust dscp**: Indicates that the DSCP values of received packets are trusted

display qos-interface traffic-limit

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-limit**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose traffic policing configuration is to be displayed.

unit-id: Unit ID of a switch, whose traffic policing configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-limit** command to display the traffic policing configuration of a port or all the ports on the device. This command also displays the traffic policing statistics.

Related commands: **traffic-limit**.

Examples

Display the traffic policing configuration and the traffic policing statistics of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 traffic-limit

GigabitEthernet1/0/1: traffic-limit
 Inbound:
   Matches: Acl 2001 rule 0  running
     Target rate: 128 Kbps
     Conform action: remark-cos video
     Exceed action: drop
   meter-statistic running
     62284 byte outprofile
     82521 byte inprofile
```

Table 1-5 display qos-interface traffic-limit command output description

Field	Description
GigabitEthernet1/0/1: traffic-limit	Port with traffic policing configured.
Inbound	Indicates that traffic policing is applied in the inbound direction.
Matches	Match criteria.
Target rate	Rate limit for traffic policing.
Conform action	Action to take on packets conforming to the rate limit, which can be: • remark-dscp *dscp-value*: Resets the DSCP value for the packets. The *dscp-value* argument can be a number in the range of 0 to 63 or a keyword shown in Table 1-17. • remark-cos *cos-value*: Resets the 802.1p precedence value for the packets. The *cos-value* argument can be a number in the range of 0 to 7 or a keyword shown in Table 1-32.
Exceed action	Action to take on the packets exceeding the rate limit, which can be: • **drop**: Drops the packets. • **forward**: Forwards the packets. • **remark-dscp** *dscp-value*: Re-marks the DSCP value of the packets. The *dscp-value* argument can be a number in the range of 0 to 63 or a keyword shown in Table 1-17. • **remark-cos** *cos-value*: Re-marks the 802.1p precedence value of the packets. The *cos-value* argument can be a number in the range of 0 to 7 or a keyword shown in Table 1-32.
meter-statistic running	Status of the function of collecting traffic policing statistics, which can be: • meter-statistic not running: Indicates that the function is not enabled. • meter-statistic running: Indicates that the function is enabled.
62284 byte outprofile	Size of the packets exceeding the rate limit (in bytes).
82521 byte inprofile	Size of the packets conforming to the rate limit (in bytes).

display qos-interface traffic-priority

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-priority**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose priority marking configuration is to be displayed.

unit-id: Unit ID of a switch, whose priority marking configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-priority** command to display the priority marking configuration of a port or all the ports on the device.

Related commands: **traffic-priority**.

Examples

Display the priority marking configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 traffic-priority
GigabitEthernet1/0/1: traffic-priority
 Inbound:
   Matches: Acl 2000 rule 0  running
     Priority action: cos controlled-load
```

Table 1-6 display qos-interface traffic-priority command output description

Field	Description
GigabitEthernet1/0/1	Port with priority marking configured.
Inbound	Indicates that priority marking is applied in the inbound direction.
Matches	Match criteria.
Priority action	Priority marking action, which can be: • cos: Indicates that the CoS precedence is marked for packets; at the same time, the marked CoS precedence value (a number in the range of 0 to 7 or a keyword shown in Table 1-32) is also displayed. • dscp: Indicates that the DSCP value is marked for packets; at the same time, the marked DSCP value (a number in the range of 0 to 63 or a keyword shown in Table 1-17) is also displayed.

display qos-interface traffic-redirect

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-redirect**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose traffic redirecting configuration is to be displayed.

unit-id: Unit ID of a switch, whose traffic redirecting configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-redirect** command to display the traffic redirecting configuration of a port or all the ports on the device.

Related commands: **traffic-redirect**.

Examples

Display the traffic redirecting configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 traffic-redirect
GigabitEthernet1/0/1: traffic-redirect
 Inbound:
   Matches: Acl 2000 rule 0  running
     Redirected to: interface GigabitEthernet1/0/2
```

Table 1-7 display qos-interface traffic-redirect command output description

Field	Description
GigabitEthernet1/0/1	Port with traffic redirecting configured.
Inbound	Indicates traffic directing is applied in the inbound direction.
Matches	Match criteria.
Redirected to	Destination port.

display qos-interface traffic-remark-vlanid

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-remark-vlanid**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose VLAN mapping configuration is to be displayed.

unit-id: Unit ID of a switch, whose VLAN mapping configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-remark-vlanid** command to display the VLAN mapping configuration of a port or all the ports on the device.

Related commands: **traffic-remark-vlanid**.

Examples

Display the VLAN mapping configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 traffic-remark-vlanid
GigabitEthernet1/0/1: traffic-remark-vlanid
 Inbound:
   Matches: Acl 2000 rule 0  running
     Remark vlan: 2
     Packet type: untagged-packet
```

Table 1-8 display qos-interface traffic-remark-vlanid command output description

Field	Description
GigabitEthernet1/0/1	Port with VLAN mapping configured.
Inbound	Indicates that VLAN mapping is applied in the inbound direction.
Matches	Match criteria.
Remark vlan	Target VLAN ID of the VLAN mapping function.
Packet type	Type of packets to which VLAN mapping applies, which can be: • **all-packet**: Performs VLAN mapping for all the packets matching the specified ACL rule. • **tagged-packet**: Performs VLAN mapping for only the tagged packets matching the specified ACL rule. • **untagged-packet**: Performs VLAN mapping for only the untagged packets matching the specified ACL rule.

display qos-interface traffic-shape

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-shape**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose traffic shaping configuration is to be displayed.

unit-id: Unit ID of a switch, whose traffic shaping configuration is to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-shape** command to display the traffic shaping configuration of a port or all the ports on the device.

Related commands: **traffic-shape**.

Examples

Display the traffic shaping configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface Gigabitethernet1/0/1 traffic-shape

 GigabitEthernet1/0/1 Port Shaping: Enable
 2000 kbps, 160 burst
 QID:    status    max-rate(kbps)   burst-size(byte)
-----------------------------------------------------
  0 :   Disable           0                 0
  1 :   Disable           0                 0
  2 :   Disable           0                 0
  3 :   Disable           0                 0
  4 :   Disable           0                 0
  5 :   Disable           0                 0
  6 :   Disable           0                 0
  7 :   Disable           0                 0
```

Table 1-9 display qos-interface traffic-shape command output description

Field	Description
GigabitEthernet1/0/1	Status of traffic shaping on the port, which can be: • Enable: Performs traffic shaping for all traffic on the port. • Disable: Performs traffic shaping for traffic of specific queues on the port.
2000 kbps	Maximum rate of all traffic on the port.
160 burst	Burst size of all traffic on the port.
QID	Queue ID.
status	Status of traffic shaping for a queue, which can be: • Enable: Indicates that queue-based traffic shaping is enabled for the queue. • Disable: Indicates that queue-based traffic shaping is disabled for the queue.
max-rate(kbps)	Maximum traffic rate of a port queue.
burst-size(byte)	Burst size of a port queue.

display qos-interface traffic-statistic

Syntax

display qos-interface { *interface-type interface-number* | *unit-id* } **traffic-statistic**

View

Any view

Parameters

interface-type interface-number: Specifies the type and number of a port, whose traffic accounting configuration and collected traffic statistics are to be displayed.

unit-id: Unit ID of a switch, whose traffic accounting configuration and collected traffic statistics are to be displayed. The *unit-id* argument is always 1.

Description

Use the **display qos-interface traffic-statistic** command to display the traffic accounting configuration and collected traffic statistics of a port or all the ports on the device.

Related commands: **traffic-statistic**.

Examples

Display the traffic accounting configuration and collected traffic statistics for GigabitEthernet 1/0/1.

```
<Sysname> display qos-interface GigabitEthernet 1/0/1 traffic-statistic
GigabitEthernet1/0/1: traffic-statistic
 Inbound:
   Matches: Acl 2000 rule 0  running
     8251 packet
```

Table 1-10 display qos-interface traffic-statistic command output description

Field	Description
GigabitEthernet1/0/1	Port with traffic accounting configured.
Inbound	Indicates that traffic accounting is applied in the inbound direction.
Matches	Match criteria.
8251 packet	The number of matched packets.

display qos-port-group

Syntax

display qos-port-group [*group-id*] { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }

View

Any view

Parameters

group-id: Port group ID, in the range 1 to 100. If no port group is specified, the specified QoS configurations of all port groups are displayed.

all: Displays all the QoS configurations of a port group.

traffic-limit: Displays the traffic policing configuration and traffic policing statistics for a port group.

traffic-priority: Displays the priority marking configuration of a port group.

traffic-redirect: Displays the traffic redirecting configuration of a port group.

traffic-statistics: Displays the traffic accounting configuration and collected traffic statistics for a port group.

Description

Use the **display qos-port-group** command to display the specified QoS configurations of a port group or all port groups.

Related commands: **mirrored-to**, **traffic-limit**, **traffic-priority, traffic-redirect**, **traffic-statistic**.

Examples

Display all the QoS configurations of port group 1.

```
<Sysname> display qos-port-group 1 all
Port-group 1 traffic-limit
 Inbound:
   Matches: Acl 3001 rule 0  running
     Target rate: 128 Kbps
     Exceed action: drop
   meter-statistic not running
```

Table 1-11 display qos-port-group command output description

Field	Description
Port-group 1	QoS features configured on the port group, which can be: • traffic-limit: Traffic policing configuration. For description on fields related to this feature, refer to Table 1-5. • traffic-priority: Priority marking configuration. For description on fields related to this feature, refer to Table 1-6. • traffic-redirect: Traffic redirecting configuration. For description on fields related to this feature, refer to Table 1-7. • traffic-statistic: Traffic accounting configuration. For description on fields related to this feature, refer to Table 1-10. • mirrored-to: Traffic mirroring configuration. For description on fields related to this feature, refer to Table 1-3.

display qos-vlan

Syntax

display qos-vlan [*vlan-id*] { **all** | **mirrored-to** | **traffic-limit** | **traffic-priority** | **traffic-redirect** | **traffic-statistic** }

View

Any view

Parameters

vlan-id: VLAN ID, in the range 1 to 4094. If no VLAN is specified, the specified QoS configurations of all VLANs are displayed.

all: Displays all the QoS configurations of a VLAN.

traffic-limit: Displays the traffic policing configuration and traffic policing statistics for a VLAN.

traffic-priority: Displays the priority marking configuration of a VLAN.

traffic-redirect: Displays the traffic redirecting configuration of a VLAN.

traffic-statistics: Displays the traffic accounting configuration and collected traffic statistics for a VLAN.

Description

Use the **display qos-vlan** command to display the specified QoS configurations of a VLAN.

Related commands: **mirrored-to**, **traffic-limit**, **traffic-priority, traffic-redirect**, **traffic-statistic**.

Examples

Display all the QoS configurations of VLAN 1 (assuming that the current device is a Switch 4200G).

```
<Sysname> display qos-vlan 1 all
Vlan 1 traffic-limit
 Inbound:
   Matches: Acl 3001 rule 0  running
     Target rate: 128 Kbps
     Exceed action: drop
   meter-statistic not running
```

Table 1-12 display qos-vlan command output description

Field	Description
Vlan 1	QoS features configured for VLAN 1, including: • traffic-limit: Traffic policing configuration. For description on fields related to this feature, refer to Table 1-5. • traffic-priority: Priority marking configuration. For description on fields related to this feature, refer to Table 1-6. • traffic-redirect: Traffic redirecting configuration. For description on fields related to this feature, refer to Table 1-7. • traffic-statistic: Traffic accounting configuration. For description on fields related to this feature, refer to Table 1-10. • mirrored-to: Traffic mirroring configuration. For description on fields related to this feature, refer to Table 1-3.

display queue-scheduler

Syntax

display queue-scheduler

View

Any view

Parameters

None

Description

Use the **display queue-scheduler** command to display the queue scheduling algorithms in use and related parameters.

Related commands: **queue-scheduler**.

Examples

Display the queue scheduling algorithms in use and related parameters on a Switch 4200G.

```
<Sysname> display queue-scheduler
QID:   scheduling-group     weight
---------------------------------
  0 :   wrr , group2           20
  1 :   wrr , group2           20
  2 :   wrr , group2           40
  3 :   wrr , group1           20
  4 :   wrr , group1           20
  5 :   wrr , group1           30
  6 :   sp                      0
  7 :   sp                      0
```

Table 1-13 display queue-scheduler command output description

Field	Description
QID	Queue ID.
scheduling-group	The queue scheduling algorithm used by each queue, which can be: • SP: Indicates that the queue uses the SP queuing. • wrr , group1: Indicates that the queue uses SDWRR and belongs to WRR group 1. • wrr , group2: Indicates that the queue uses SDWRR and belongs to WRR group 1.
weight	Weight of the queue.

mirrored-to

Syntax

mirrored-to inbound *acl-rule* **monitor-interface**

undo mirrored-to inbound *acl-rule*

View

System view, port group view, Ethernet port view

Parameters

inbound: Mirrors incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

Table 1-14 Ways of applying combined ACL rules

ACL combination	Form of the *acl-rule* argument
Apply a basic or advanced Layer 3 ACL	**ip-group** *acl-number*
Apply a rule of a Layer 3 ACL	**ip-group** *acl-number* **rule** *rule-id*
Apply all the rules of a Layer 2 ACL	**link-group** *acl-number*
Apply a rule of a Layer 2 ACL	**link-group** *acl-number* **rule** *rule-id*
Apply all the rules in an IPv6 ACL	**user-group** *acl-number*
Apply a rule in an IPv6 ACL	**user-group** *acl-number* **rule** *rule-id*
Apply a rule of a Layer 3 ACL and a rule of a Layer 2 ACL	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

Table 1-15 Description on the parameters in Table 1-14

Parameters	Description
ip-group *acl-number*	Specifies the number of a basic or advanced ACL, in the range 2000 to 3999.
link-group *acl-number*	Specifies the number of a Layer 2 ACL, in the range 4000 to 4999.
user-group *acl-number*	IPv6 ACL number, in the range 5000 to 5999.
rule-id	ACL rule number, in the range 0 to 65534. If the *rule-id* argument is not provided, all rules of the ACL are specified.

monitor-interface: Mirrors the packets to the monitor port.

Description

Use the **mirrored-to** command to configure mirroring the incoming packets matching the specific ACL rules to the monitor port globally, in a port group, or on a port.

Use the **undo mirrored-to** command to remove a traffic mirroring action configured globally, on a port, or in a port group.

Related commands: **display qos-interface mirrored-to**.

Examples

Mirror the incoming packets matching ACL 2000 to GigabitEthernet 1/0/4 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/4
[Sysname- GigabitEthernet1/0/4] monitor-port
[Sysname- GigabitEthernet1/0/4] quit
```

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirrored-to inbound ip-group 2000 monitor-interface
```

mirrored-to vlan

Syntax

mirrored-to vlan *vlan-id* **inbound** *acl-rule* **monitor-interface**

undo mirrored-to vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Mirrors incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

monitor-interface: Mirrors the packets to the monitor port.

Description

Use the **mirrored-to vlan** command to mirror the incoming packets matching the specific ACL rules in a specific VLAN to the specified monitor port.

Use the **undo mirrored-to vlan** command to remove the configuration.

Related commands: **display qos-vlan**.

Examples

Mirror the incoming packets matching ACL 2000 in VLAN 1 to GigabitEthernet 1/0/2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] monitor-port
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] mirrored-to vlan 1 inbound ip-group 2000 monitor-interface
```

monitor-port

Syntax

monitor-port

undo monitor-port

View

Ethernet port view

Parameters

None

Description

Use the **monitor-port** command to configure a port as the monitor port for traffic mirroring.

Use the **undo monitor-port** command to remove the configuration.

Note that link aggregation group member ports, LACP-enabled ports, and STP-enabled ports cannot be configured as monitor ports.

Note

When you configure an Ethernet port as a monitor port, if local mirroring group 1 does not exist, the device automatically creates local mirroring group 1 and adds the monitor port to the mirroring group; if mirroring group 1 already exists and is configured as a remote mirroring group, your monitor port configuration will fail.

Examples

Configure GigabitEthernet1/0/4 as the monitor port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] monitor-port
```

priority

Syntax

priority *priority-level*

undo priority

View

Ethernet port view

Parameters

priority-level: Port priority, ranging from 0 to 7.

Description

Use the **priority** command to configure the priority of an Ethernet port.

Use the **undo priority** command to restore the priority of an Ethernet port to the default.

By default, the priority of an Ethernet port is 0.

With the **priority** command configured on a port, the switch takes the configured port priority of the port as the 802.1p precedence value of the received packet, searches for the precedence values corresponding to the 802.1p precedence value in the CoS-precedence-to-other-precedence mapping table, and assigns the matching precedence values to the packet.

Examples

Set the priority of GigabitEthernet 1/0/1 to 6.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] priority 6
```

priority-trust

Syntax

priority-trust { **cos** [**automap**] | **dscp** [**automap** | **remap**] }

undo priority-trust

View

Ethernet port view

Parameters

cos [**automap**]: Configured to use the 802.1p precedence carried in the incoming traffic for priority mapping and decide how the switch processes the DSCP field when delivering the traffic:

- If **automap** is not specified (the default), the switch keeps the original DSCP value of the traffic unchanged.
- If **automap** is specified, the switch replaces the original DSCP value carried in the incoming traffic with the target DSCP value.

dscp [**automap** | **remap**]: Configured to use the DSCP value carried in the incoming traffic for priority mapping and decide how the switch processes the CoS field when delivering the traffic:

- If neither **automap** nor **remap** is specified, the switch keeps the original 802.1p precedence value of the incoming traffic unchanged.
- With **automap** specified, the switch replaces the original 802.1p precedence value of the incoming traffic with the target one.
- If **remap** is specified, the switch looks up the DSCP-to-DSCP mapping table for the DSCP value corresponding to the DSCP value carried in the incoming traffic, then searches for the set of precedence values corresponding to the new DSCP value in the DSCP-to-other-precedence mapping table, and then replaces the 802.1p precedence value of the traffic with the target one.

Description

Use the **priority-trust** command to specify the trusted priority type and packet processing mode on an Ethernet port.

Use the **undo priority-trust** command to restore the default.

An Ethernet port trusts the port priority by default.

Related commands: **display qos-interface priority-trust**.

Examples

Configure the switch to trust 802.1p precedence of received packets and use the default packet processing mode on GigabitEthernet 1/0/1.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] priority-trust cos
```

protocol-priority protocol-type

Syntax

protocol-priority protocol-type *protocol-type* { **ip-precedence** *ip-precedence* | **dscp** *dscp-value* }

undo protocol-priority protocol-type *protocol-type*

View

System view

Parameters

protocol-type *protocol-type*: Specifies the protocol type, which can be Telnet, SNMP, or ICMP.

ip-precedence *ip-precedence*: Specifies an IP precedence value, in the range 0 to 7. Alternatively, you can enter a keyword listed in Table 1-16 as the IP precedence value.

Table 1-16 IP precedence keywords and the corresponding decimal/binary values

Keyword	IP precedence value (decimal)	IP precedence value (binary)
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

dscp *dscp-value*: Specifies the DSCP value, in the range of 0 to 63. Alternatively, you can enter a keyword listed in Table 1-17 as the DSCP value.

Table 1-17 DSCP value keywords and the corresponding decimal/binary values

Keyword	DSCP value (decimal)	DSCP value (binary)
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010

Keyword	DSCP value (decimal)	DSCP value (binary)
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
be (the default)	0	000000
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
ef	46	101110

Description

Use the **protocol-priority** command to set an IP precedence value or DSCP value for locally generated packets of a specific protocol globally.

Use the **undo protocol-priority** command to remove the IP precedence value or DSCP value set for the locally generated packets of a specific protocol globally.

Related commands: **display protocol-priority**.

Examples

Set the IP precedence value to 3 for SNMP protocol packets.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] protocol-priority protocol-type snmp ip-precedence 3
```

qos cos-drop-precedence-map

Syntax

qos cos-drop-precedence-map *cos0-map-drop-prec cos1-map-drop-prec cos2-map-drop-prec cos3-map-drop-prec cos4-map-drop-prec cos5-map-drop-prec cos6-map-drop-prec cos7-map-drop-prec*

undo qos cos-drop-precedence-map

View

System view

Parameters

cos0-map-drop-prec: Drop precedence value to which CoS 0 is to be mapped, in the range 0 to 1.

cos1-map-drop-prec: Drop precedence value to which CoS 1 is to be mapped, in the range 0 to 1.

cos2-map-drop-prec: Drop precedence value to which CoS 2 is to be mapped, in the range 0 to 1.

cos3-map-drop-prec: Drop precedence value to which CoS 3 is to be mapped, in the range 0 to 1.

cos4-map-drop-prec: Drop precedence value to which CoS 4 is to be mapped, in the range 0 to 1.

cos5-map-drop-prec: Drop precedence value to which CoS 5 is to be mapped, in the range 0 to 1.

cos6-map-drop-prec: Drop precedence value to which CoS 6 is to be mapped, in the range 0 to 1.

cos7-map-drop-prec: Drop precedence value to which CoS 7 is to be mapped, in the range 0 to 1.

Description

Use the **qos cos-drop-precedence-map** command to modify the CoS-precedence-to-drop-precedence mapping table.

Use the **undo qos cos-drop-precedence-map** command to restore the default CoS-precedence-to-drop-precedence mapping table.

Table 1-18 shows the default CoS-precedence-to-drop-precedence mapping table.

Table 1-18 The default CoS-precedence-to-drop-precedence mapping table

CoS value	Drop precedence value
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Related commands: **display qos cos-drop-precedence-map**.

Examples

Modify the CoS-precedence-to-drop-precedence mapping table according to Table 1-19.

Table 1-19 A CoS-precedence-to-drop-precedence mapping table

CoS value	Drop precedence value
0	1
1	1
2	1
3	1
4	1

CoS value	Drop precedence value
5	0
6	0
7	0

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos cos-drop-precedence-map 1 1 1 1 1 0 0 0
```

qos cos-dscp-map

Syntax

qos cos-dscp-map *cos0-map-dscp cos1-map-dscp cos2-map-dscp cos3-map-dscp cos4-map-dscp cos5-map-dscp cos6-map-dscp cos7-map-dscp*

undo qos cos- dscp-map

View

System view

Parameters

cos0-map-dscp: DSCP value to which CoS 0 is to be mapped, in the range 0 to 63.

cos1-map-dscp: DSCP value to which CoS 1 is to be mapped, in the range 0 to 63.

cos2-map-dscp: DSCP value to which CoS 2 is to be mapped, in the range 0 to 63.

cos3-map-dscp: DSCP value to which CoS 3 is to be mapped, in the range 0 to 63.

cos4-map-dscp: DSCP value to which CoS 4 is to be mapped, in the range 0 to 63.

cos5-map-dscp: DSCP value to which CoS 5 is to be mapped, in the range 0 to 63.

cos6-map-dscp: DSCP value to which CoS 6 is to be mapped, in the range 0 to 63.

cos7-map-dscp: DSCP value to which CoS 7 is to be mapped, in the range 0 to 63.

Description

Use the **qos cos-dscp-map** command to modify the CoS-precedence-to-DSCP mapping table.

Use the **undo qos cos-dscp-map** command to restore the default CoS-precedence-to-DSCP mapping table.

Table 1-20 shows the default CoS-precedence-to-DSCP mapping table.

Table 1-20 The default CoS-precedence-to-DSCP mapping table

CoS value	DSCP value
0	16
1	0
2	8
3	24

CoS value	DSCP value
4	32
5	40
6	48
7	56

Related commands: **display qos cos-dscp-map**.

Examples

Modify the CoS-precedence-to-DSCP mapping table according to Table 1-21.

Table 1-21 A CoS-precedence-to-DSCP mapping table

CoS value	DSCP value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos cos-dscp-map 0 1 2 3 4 5 6 7
```

qos cos-local-precedence-map

Syntax

qos cos-local-precedence-map *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*

undo qos cos-local-precedence-map

View

System view

Parameters

cos0-map-local-prec: Local precedence value to which CoS 0 is to be mapped, in the range 0 to 7.

cos1-map-local-prec: Local precedence value to which CoS 1 is to be mapped, in the range 0 to 7.

cos2-map-local-prec: Local precedence value to which CoS 2 is to be mapped, in the range 0 to 7.

cos3-map-local-prec: Local precedence value to which CoS 3 is to be mapped, in the range 0 to 7.

cos4-map-local-prec: Local precedence value to which CoS 4 is to be mapped, in the range 0 to 7.

cos5-map-local-prec: Local precedence value to which CoS 5 is to be mapped, in the range 0 to 7.

cos6-map-local-prec: Local precedence value to which CoS 6 is to be mapped, in the range 0 to 7.

cos7-map-local-prec: Local precedence value to which CoS 7 is to be mapped, in the range 0 to 7.

Description

Use the **qos cos-local-precedence-map** command to modify the CoS-precedence-to-local-precedence mapping table.

Use the **undo qos cos-local-precedence-map** command to restore the default CoS-precedence-to-local-precedence mapping table.

As the port of a Switch 4200G can accommodate up to eight output queues, as shown in Table 1-22.

Table 1-22 The default CoS-precedence-to-local-precedence mapping table on Switch 4200G series

CoS value	Local precedence value
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Related commands: **display qos cos-local-precedence-map**.

Examples

Modify the CoS-precedence-to-local-precedence mapping table according to Table 1-23.

Table 1-23 A CoS-precedence-to-local-precedence mapping table

CoS value	Local precedence value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos cos-local-precedence-map 0 1 2 3 4 5 6 7
```

qos dscp-cos-map

Syntax

qos dscp-cos-map *dscp-list* **:** *cos-value*

undo qos dscp-cos-map [*dscp-list*]

View

System view

Parameters

dscp-list: A DSCP value or multiple DSCP values each separated by a space. The value range for DSCP values is 0 to 63. The *dscp-list* argument is separated from the *cos-value* argument by a colon (:).

cos-value: 802.1p precedence value, in the range of 0 to 7. It is mapped to the specified DSCP value or values.

Description

Use the **qos dscp-cos-map** command to modify the DSCP-to-CoS-precedence mapping table.

Use the **undo qos dscp-cos-map** command to restore the default DSCP-to-CoS-precedence mapping table.

Table 1-24 shows the default DSCP-to-CoS-precedence mapping table.

Table 1-24 The default DSCP-to-CoS-precedence mapping table

DSCP value range	CoS value
0 to 7	1
8 to 15	2
16 to 23	0
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Related commands: **display qos dscp-cos-map**.

Examples

Modify the DSCP-to-CoS-precedence mapping table according to Table 1-25.

Table 1-25 A DSCP-to-CoS-precedence mapping table

DSCP values	CoS value
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos dscp-cos-map 0 1 2 3 4 5 6 7 : 0
[Sysname] qos dscp-cos-map 8 9 10 11 12 13 14 15 : 1
[Sysname] qos dscp-cos-map 16 17 18 19 20 21 22 23 : 2
[Sysname] qos dscp-cos-map 24 25 26 27 28 29 30 31 : 3
[Sysname] qos dscp-cos-map 32 33 34 35 36 37 38 39 : 4
[Sysname] qos dscp-cos-map 40 41 42 43 44 45 46 47 : 5
[Sysname] qos dscp-cos-map 48 49 50 51 52 53 54 55 : 6
[Sysname] qos dscp-cos-map 56 57 58 59 60 61 62 63 : 7
```

qos dscp-drop-precedence-map

Syntax

qos dscp-drop-precedence-map *dscp-list* **:** *drop-precedence*

undo qos dscp-drop-precedence-map [*dscp-list*]

View

System view

Parameters

dscp-list: A DSCP value or multiple DSCP values each separated by a space. The value range for DSCP values is 0 to 63. The *dscp-list* argument is separated from the *drop-precedence* argument by a colon (:).

drop-precedence: Drop precedence value, in the range of 0 to 1. It is mapped to the specified DSCP value or values.

Description

Use the **qos dscp-drop-precedence-map** command to modify the DSCP-to-drop-precedence mapping table.

Use the **undo qos dscp-drop-precedence-map** command to restore the default DSCP-to-drop-precedence mapping table.

Table 1-26 shows the default DSCP-to-drop-precedence mapping table.

Table 1-26 The default DSCP-to-drop-precedence mapping table

DSCP value range	Drop precedence value
0 to 7	1
8 to 15	1
16 to 23	1
24 to 31	1
32 to 39	0
40 to 47	0
48 to 55	0
56 to 63	0

Related commands: **display qos dscp-drop-precedence-map**.

Examples

Modify the DSCP-to-drop-precedence mapping table according to Table 1-27.

Table 1-27 A DSCP-to-drop-precedence mapping table

DSCP value range	Drop precedence value
0 to 7	0
8 to 15	1
16 to 23	1
24 to 31	1
32 to 39	0
40 to 47	0
48 to 55	0
56 to 63	0

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos dscp-drop-precedence-map 0 1 2 3 4 5 6 7 : 0
```

qos dscp-dscp-map

Syntax

qos dscp-dscp-map *dscp-list* **:** *dscp-value*

undo qos dscp-dscp-map [*dscp-list*]

View

System view

Parameters

dscp-list: A DSCP value or multiple DSCP values each separated by a space. The value range for DSCP values is 0 to 63. The *dscp-list* argument is separated from the *dscp-value* argument by a colon (:).

dscp-value: A target DSCP value, in the range of 0 to 63. It is mapped to the specified DSCP value or values.

Description

Use the **qos dscp-dscp-map** command to modify the DSCP-to-DSCP mapping table.

Use the **undo qos dscp-dscp-map** command to restore the default DSCP-to-DSCP mapping table.

Table 1-28 shows the default DSCP-to-DSCP mapping table.

Table 1-28 The default DSCP-to-DSCP mapping table

Source DSCP value	Target DSCP value
0	0
1	1
2	2
...	...
61	61
62	62
63	63

Related commands: **display qos dscp-dscp-map**.

Examples

Modify the DSCP-to-DSCP mapping table according to Table 1-29.

Table 1-29 A DSCP-to-DSCP mapping table

Source DSCP value	Target DSCP value
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	8

Source DSCP value	Target DSCP value
9	9
10	10
...	...
61	61
62	62
63	63

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos dscp-dscp-map 0 1 2 3 4 5 6 7 : 1
```

qos dscp-local-precedence-map

Syntax

qos dscp-local-precedence-map *dscp-list* **:** *local-precedence*

undo qos dscp-local-precedence-map [*dscp-list*]

View

System view

Parameters

dscp-list: A DSCP value or multiple DSCP values each separated by a space. The value range for DSCP values is 0 to 63. The *dscp-list* argument is separated from the *local-precedence* argument by a colon (:).

local-precedence: Local precedence value mapped to the specified DSCP value or values. This argument is in the range of 0 to 7 on the Switch 4200G series.

Description

Use the **qos dscp-local-precedence-map** command to modify the DSCP-to-local-precedence mapping table.

Use the **undo qos dscp-local-precedence-map** command to restore the default DSCP-to-local-precedence mapping table.

As the port of a Switch 4200G can accommodate up to eight output queues, as shown in Table 1-30.

Table 1-30 The default DSCP-to-local-precedence mapping table on the Switch 4200G series

DSCP value range	Local precedence value
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3

DSCP value range	Local precedence value
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Related commands: **display qos dscp-local-precedence-map**.

Examples

Modify the DSCP-to-local-precedence mapping table according to Table 1-31.

Table 1-31 A DSCP-to-local-precedence mapping table

DSCP values	Local precedence value
0 to 7	1
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

The configuration procedure is as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos dscp-local-precedence-map 0 1 2 3 4 5 6 7 : 1
```

queue-scheduler

Syntax

queue-scheduler wrr { **group1** { *queue-id queue-weight* } &<1-8> | **group2** { *queue-id queue-weight* } &<1-8> }*

undo queue-scheduler [*queue-id*] &<1-8>

View

System view

Parameters

wrr: Uses the shaped deficit weighted round robin (SDWRR) queuing.

group1: Assigns the specified queues to WRR scheduling group 1.

group2: Assigns the specified queues to WRR scheduling group 2.

queue-id: Queue ID, in the range 0 to 7.

queue-weight: Weight assigned to a queue, in the range 1 to 255.

&<1-8>: Indicates that the *queue-id* argument and the *queue-weight* argument can be entered for up to eight times.

Description

Use the **queue-scheduler** command to specify the queue scheduling algorithms to be used and the related parameters for the specific queues.

Use the **undo queue-scheduler** command to restore the default.

By default, the SP queuing is used.

The port of a Switch 4200G can accommodate up to eight. You can configure to use SP queuing, SDWRR queuing, or SP queuing in combination with SDWRR queuing as required.

- With SDWRR queuing adopted, the output queues of a port can be assigned to group 1 and group 2. The two groups are scheduled using the SP algorithm. For example, you can assign queues 0 through 3 to group 1, and assign queues 4 through 7 to group 2. The queues in group 2 are scheduled preferentially using WRR. The queues in group 1 are scheduled using WRR only when all the queues in group 2 are empty.
- With both SP queuing and SDWRR queuing adopted, groups are scheduled using the SP algorithm. Assume that queue 0 and queue 1 are scheduled using SP queuing, queues 2 through 4 are assigned to group 1, and queues 5 through 7 are assigned to group 2. The queues in group 2 are scheduled preferentially using WRR. When all the queues in group 2 are empty, the queues in group 1 are scheduled using WRR. Then, queue 1 is scheduled, and then queue 0.

Note

When using SDWRR or SP-SDWRR combination for queue scheduling, you are recommended to assign queues with successive queue numbers to the same scheduling group.

Related commands: **display queue-scheduler**.

Examples

Use both SP and SDWRR for queue scheduling, assigning queue 3, queue 4, and queue 5 to WRR scheduling group 1, with the weigh of 20, 20 and 30; assigning queue 0, queue 1, and queue 2 to WRR scheduling group 2, with the weight 20, 20, and 40; and scheduling queue 6 and queue 7 using the SP algorithm.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] queue-scheduler wrr group1 3 20 4 20 5 30 group2 0 20 1 20 2 40
[Sysname] display queue-scheduler
 QID:   scheduling-group     weight
-----------------------------------
  0 :   wrr , group2           20
  1 :   wrr , group2           20
  2 :   wrr , group2           40
  3 :   wrr , group1           20
```

```
4 :   wrr , group1          20
5 :   wrr , group1          30
6 :   sp                     0
7 :   sp                     0
```

reset traffic-limit

Syntax

reset traffic-limit inbound *acl-rule*

View

System view, Ethernet port view, port group view

Parameters

inbound: Clears the statistics about the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15.

Description

Use the **reset traffic-limit** command to clear the traffic policing statistics of the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Related commands: **traffic-limit**.

Examples

Clear the traffic policing statistics of the incoming packets matching ACL 2000 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] reset traffic-limit inbound ip-group 2000
```

reset traffic-limit vlan

Syntax

reset traffic-limit vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Clears the statistics about the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15.

Description

Use the **reset traffic-limit vlan** command to clear the statistics of the incoming packets matching the specific ACL rules in a VLAN.

Related commands: **traffic-limit vlan**.

Examples

Clear the statistics of the incoming packets matching ACL 2000 in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] reset traffic-limit vlan 1 inbound ip-group 2000
```

reset traffic-statistic

Syntax

reset traffic-statistic inbound *acl-rule*

View

System view, Ethernet port view, port group view

Parameters

inbound: Clears statistics about the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15.

Description

Use the **reset traffic-statistics** command to clear the statistics about the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Related commands: **traffic-statistic**.

Examples

Clear the statistics about the incoming packets matching ACL 2000 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] reset traffic-statistic inbound ip-group 2000
```

reset traffic-statistic vlan

Syntax

reset traffic-statistic vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Clears the statistics about the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15.

Description

Use the **reset traffic-statistics vlan** command to clear the statistics about the incoming packets matching the specific ACL rules for the specified VLAN.

Related commands: **traffic-statistic vlan**.

Examples

Clear the statistics on packets incoming packets matching ACL 2000 in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] reset traffic-statistic vlan 1 inbound ip-group 2000
```

traffic-limit

Syntax

traffic-limit inbound *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]

undo traffic-limit inbound *acl-rule* [**meter-statistic**]

View

System view, Ethernet port view, port group view

Parameters

inbound: Performs traffic policing on incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

target-rate: Rate limit of traffic policing (in kbps). This argument is in the range of 1 to 44000000 in system view and port group view. In Ethernet port view, the range of this argument varies by port type as follows:

- Gigabit port: In the range 1 to 1000000
- 10G port: In the range 1 to 10000000

conform *con-action*: Specifies the action to take on the packets conforming to the rate limit in addition to the action of forwarding. The *con-action* argument can be:

- **remark-dscp** *dscp-value*: Re-sets the DSCP value for the packets. The *dscp-value* argument is in the range of 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value* : Re-sets the 802.1p precedence value for the packets. The *cos-value* argument is in the range of 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

Table 1-32 802.1p precedence keywords and the corresponding decimal/binary values

Keyword	802.1p precedence value (decimal)	802.1p precedence value (binary)
best-effort	0	000
background	1	001
Spare	2	010
excellent-effort	3	011
controlled-load	4	100
Video	5	101
Voice	6	110
Network-management	7	111

exceed *exceed-action*: Specifies the action to take on the packets exceeding the rate limit. The action can be:

- **drop**: Drops the packets.
- **forward**: Forwards the packets.
- **remark-dscp** *dscp-value*: Resets the DSCP value of the packets and forwards them at the same time. The DSCP value is in the range of 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value*: Resets the 802.1p precedence value of the packets and forwards them at the same time. The *cos-value* argument is in the range of 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

meter-statistic: Collects traffic policing statistics. It can measure in bytes the traffic conforming to the rate limit and the traffic exceeding the rate limit.

Description

Use the **traffic-limit** command to configure traffic policing for the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Use the **undo traffic-limit** command to remove the configuration.

The granularity of traffic policing is described in Table 1-33:

Table 1-33 The granularity of traffic policing

Rate limit range	Granularity
0 to 1 Mbps	1 kbps
0 to 10 Mbps	10 kbps
0 to 100 Mbps	100 kbps
0 to 1 Gbps	1 Mbps
0 to 10 Gbps	10 Mbps

Related commands: **display qos-interface traffic-limit**.

Examples

Perform traffic policing for incoming packets matching ACL 4000 on GigabitEthernet 1/0/1, limiting the rate to 128 kbps and dropping the packets exceeding the rate limit.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-limit inbound link-group 4000 128 exceed drop
```

traffic-limit vlan

Syntax

traffic-limit vlan *vlan-id* **inbound** *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]

undo traffic-limit vlan *vlan-id* **inbound** *acl-rule* [**meter-statistic**]

View

System view

Parameters

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

inbound: Performs traffic policing on the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

target-rate: Rate limit of traffic policing (in kbps). This argument is in the range 1 to 44000000.

conform *con-action*: Specifies the action to take on the packets conforming to the rate limit in addition to the action of forwarding. The action can be:

- **remark-dscp** *dscp-value*: Sets the DSCP value of the packets to the specified value. The *dscp-value* argument is in the range of 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value* : Sets the 802.1p precedence value of the packets to the specified value. The *cos-value* argument is in the range of 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

exceed *exceed-action*: Specifies the action to take on the packets exceeding the rate limit. The action can be:

- **drop**: Drops the packets.
- **forward**: Forwards the packets.
- **remark-dscp** *dscp-value*: Resets the DSCP value of the packets and forwards them at the same time. The *dscp-value* argument is in the range of 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value*: Resets the 802.1p precedence value of the packets and forwards them at the same time. The *cos-value* argument is in the range of 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

meter-statistic: Collects traffic policing statistics. It can measure in bytes the traffic conforming to the rate limit and the traffic exceeding the rate limit.

Description

Use the **traffic-limit vlan** command to configure traffic policing for a VLAN, that is, set the rate limit for the incoming packets matching the specific ACL rules in a VLAN, and specify the action to take on the conforming packets and the exceeding packets.

Use the **undo traffic-limit vlan** command to remove the configuration.

Refer to Table 1-33 for the granularity of traffic policing.

Related commands: **display qos-vlan**.

Examples

Perform traffic policing for the incoming packets matching ACL 4000 in VLAN 1, limiting the rate to 128 kbps and dropping the packets exceeding the rate limit.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] traffic-limit vlan 1 inbound link-group 4000 128 exceed drop
```

traffic-priority

Syntax

traffic-priority inbound *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }

undo traffic-priority inbound *acl-rule*

View

System view, Ethernet port view, port group view

Parameters

inbound: Performs priority marking for the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

dscp *dscp-value*: Sets the DSCP value, in the range 0 to 63. You can also enter a keyword listed in Table 1-17 for the *dscp-value* argument.

cos *cos-value*: Sets the 802.1p precedence value, in the range 0 to 7. You can also enter a keyword listed in Table 1-32 for the *cos-value* argument.

Description

Use the **traffic-priority** command to re-set the priority of the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Use the **undo traffic-priority** to remove the configuration.

Related commands: **display qos-interface traffic-priority**.

Examples

Set the 802.1p precedence value to 1 for the incoming packets matching ACL 4000 on GigabitEthernet 1/0/1.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-priority inbound link-group 4000 cos 1
```

traffic-priority vlan

Syntax

traffic-priority vlan *vlan-id* **inbound** *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }

undo traffic-priority vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Performs priority marking for the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

dscp *dscp-value*: Sets the DSCP value, in the range of 0 to 63. You can also enter a keyword listed in Table 1-17 for the *dscp-value* argument.

cos *cos-value*: Sets the 802.1p precedence value, in the range of 0 to 7. You can also enter a keyword listed in Table 1-32 for the *cos-value* argument.

Description

Use the **traffic-priority vlan** command to re-set the priority for the incoming packets matching the specific ACL rules in the specific VLAN.

Use the **undo traffic-priority vlan** to remove the configuration.

Related commands: **display qos-vlan**.

Examples

Set the 802.1p precedence value to 1 for the incoming packets matching ACL 4000 in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] traffic-priority vlan 1 inbound link-group 4000 cos 1
```

traffic-redirect

Syntax

traffic-redirect inbound *acl-rule* **interface** *interface-type interface-number*

undo traffic-redirect inbound *acl-rule*

View

System view, Ethernet port view, port group view

Parameters

inbound: Redirects the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

interface *interface-type interface-number*: Redirects packets to an Ethernet port specified by its type and number.

Description

Use the **traffic-redirect** command to redirect the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Use the **undo traffic-redirect** command to remove the configuration.

Note

If the traffic is redirected to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state. Refer to *Basic Port Configuration* module of this manual for information about Combo ports.

Related commands: **display qos-interface traffic-redirect**.

Examples

Redirect the incoming packets matching ACL 2000 on GigabitEthernet 1/0/1 to GigabitEthernet 1/0/7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1]  traffic-redirect  inbound  ip-group  2000  interface
GigabitEthernet1/0/7
```

traffic-redirect vlan

Syntax

traffic-redirect vlan *vlan-id* **inbound** *acl-rule* **interface** *interface-type interface-number*

undo traffic-redirect vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Redirects the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

interface *interface-type interface-number*: Redirects packets to an Ethernet port specified by its port and number.

Description

Use the **traffic-redirect vlan** command to redirect the incoming packets matching the specific ACL rules in a specific VLAN to a specified port.

Use the **undo traffic-redirect vlan** command to remove the configuration.

Note

If the traffic is redirected to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state. Refer to *Basic Port Configuration* module of this manual for information about Combo ports.

Related commands: **display qos-vlan**.

Examples

Redirect the incoming packets matching ACL 2000 in VLAN 1 to GigabitEthernet 1/0/7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] traffic-redirect vlan 1 inbound ip-group 2000 interface GigabitEthernet1/0/7
```

traffic-remark-vlanid

Syntax

traffic-remark-vlanid inbound *acl-rule* **remark-vlan** *vlan-id* [**all-packet** | **tagged-packet** | **untagged-packet**]

undo traffic-remark-vlanid inbound *acl-rule*

View

Ethernet port view

Parameters

inbound: Performs VLAN mapping for the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

remark-vlan *vlan-id*: Specifies the target VLAN ID to be marked for packets.

all-packet: Performs VLAN mapping for all the packets matching the specific ACL rules.

tagged-packet: Performs VLAN mapping for tagged packets matching the specific ACL rules.

untagged-packet: Performs VLAN mapping for untagged packets matching the specific ACL rules.

Description

Use the **traffic-remark-vlanid command** to enable VLAN mapping and set the target VLAN ID for the incoming packets matching the specific ACL rules on a port.

Use the **undo traffic-remark-vlanid** command to disable VLAN mapping for the incoming packets matching the specific ACL rules.

Note

Currently, the **all-packet** keyword and the **tagged-packet** keyword are not supported.

Related commands: **display qos-interface traffic-remark-vlanid**.

Examples

Configure VLAN mapping on GigabitEthernet 1/0/1 of a Switch 4200G to map the VLAN IDs of incoming packets matching ACL 4001 to 1001.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-remark-vlanid inbound link-group 4001 remark-vlan
1001
```

traffic-shape

Syntax

traffic-shape [**queue** *queue-id*] *max-rate burst-size*

undo traffic-shape [**queue** *queue-id*]

View

Ethernet port view

Parameters

queue *queue-id*: Specifies the ID of a queue, in the range of 0 to 7.

max-rate: Maximum traffic rate on a port, in kbps.

burst-size: Burst size (in KB), in the range 16 to 16000. This argument must be a multiple of 4.

Description

Use the **traffic-shape** command to configure traffic shaping on a port.

Use the **undo traffic-shape** command to disable traffic shaping on a port.

To shape all traffic on the port, do not specify the **queue** *queue-id* keyword and argument combination. To shape traffic of a specific output queue rather than of all queues on the port, specify the queue with the **queue** *queue-id* keyword.

Table 1-34 The granularity of traffic shaping

Port type	The set traffic shaping value	Granularity (in bps)
GE ports	0 to 80 Mbps	20 kbps
GE ports	80 Mbps to 1 Gbps	260 kbps
10GE ports	0 to 10 Gbps	2500 kbps

Related commands: **display qos-interface traffic-shape**.

Examples

Configure traffic shaping on GigabitEthernet 1/0/1 of a Switch 4200G, with the maximum rate being 640 kbps and the burst size being 16 KB.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-shape 640 16
```

traffic-statistic

Syntax

traffic-statistic inbound *acl-rule*

undo traffic-statistic inbound *acl-rule*

View

System view, Ethernet port view, port group view

Parameters

inbound: Collects statistics on the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

Description

Use the **traffic-statistic** command to collect statistics for the incoming packets matching the specific ACL rules globally, on a port, or in a port group.

Use the **undo traffic-statistic** command to remove the configuration.

Related commands: **display qos-interface traffic-statistic**.

Examples

Collect statistics for the incoming packets matching ACL 2000 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-statistic inbound ip-group 2000
```

traffic-statistic vlan

Syntax

traffic-statistic vlan *vlan-id* **inbound** *acl-rule*

undo traffic-statistic vlan *vlan-id* **inbound** *acl-rule*

View

System view

Parameters

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

inbound: Collects statistics for the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

Description

Use the **traffic-statistic vlan** command to collect statistics for the incoming packets matching the specific ACL rules for a specific VLAN.

Use the **undo traffic-statistic vlan** command to remove the configuration.

Related commands: **display qos-vlan**.

Examples

Collect statistics for the incoming packets matching ACL 2000 in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] traffic-statistic vlan 1 inbound ip-group 2000
```

2 QoS Profile Configuration Commands

QoS Profile Configuration Commands

apply qos-profile

Syntax

In system view

apply qos-profile *profile-name* **interface** *interface-list*

undo apply qos-profile *profile-name* **interface** *interface-list*

In Ethernet port view

apply qos-profile *profile-name*

undo apply qos-profile *profile-name*

View

System view, Ethernet port view

Parameters

profile-name: QoS profile name, a string of 1 to 32 characters and starting with English letters [a-z, A-Z].

interface-list: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-type interface-number* [**to** *interface-type interface-number*].

Description

Use the **apply qos-profile** command to apply a QoS profile to a port or multiple ports.

Use the **undo apply qos-profile** command to remove a QoS profile from a port or multiple ports.

Examples

Apply the QoS profile named **a123** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] apply qos-profile a123
```

Apply the QoS profile named **a123** to GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] apply qos-profile a123 interface GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
```

display qos-profile

Syntax

display qos-profile { **all** | **name** *profile-name* | **interface** *interface-type interface-number* | **user** *user-name* }

View

Any view

Parameters

all: Specifies all the QoS profiles.

name *profile-name*: Specifies a QoS profile name, a string of 1 to 32 characters and starting with English letters [a-z, A-Z].

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

user *user-name*: Specifies a user by its name, a string of 1 to 80 characters.

Description

Use the **display qos-profile** command to display the configuration of a QoS profile or all the QoS profiles.

Examples

Display the configuration of QoS profile **a123**.

```
<Sysname> display qos-profile name a123
qos-profile: a123, 3 actions
 traffic-limit inbound ip-group 2000 rule 0 640
 packet-filter inbound ip-group 2000 rule 0
traffic-priority inbound ip-group 2000 rule 1 cos video
```

Display the configuration of the QoS profile applied to GigabitEthernet 1/0/1, assuming that the QoS profile has been applied to GigabitEthernet 1/0/1 manually.

```
<Sysname> display qos-profile interface GigabitEthernet 1/0/1
User's qos-profile applied mode: user-based
Default applied qos-profile: a123, 3 actions
 traffic-limit inbound ip-group 2000 rule 0 640
 packet-filter inbound ip-group 2000 rule 0
traffic-priority inbound ip-group 2000 rule 1 cos video
```

Table 2-1 display qos-profile command output description

Field	Description
qos-profile: a123, 3 actions	Name of the QoS profile and the number of actions configured in the QoS profile
traffic-limit inbound ip-group 2000 rule 0 640	Limit the rate of the incoming packets matching rule 0 of ACL 2000 to 640 kbps
packet-filter inbound ip-group 2000 rule 0	Filter the incoming packets matching rule 0 of ACL 2000

Field	Description
traffic-priority inbound ip-group 2000 rule 0 cos video	Set the 802.1p precedence of the incoming packets matching rule 0 of ACL 4000 to **video** (that is, 802.1p precedence 5)
User's qos-profile applied mode	The QoS profile is dynamically applied and the application mode could be: • User-based • Port-based For detailed information about the two application modes, refer to the corresponding operation manual.
Default applied qos-profile: a123, 3 actions	"Default" indicates that the QoS profile named **a123** is applied to GigabitEthernet 1/0/1 manually. The QoS profile contains three actions.

packet-filter

Syntax

packet-filter inbound *acl-rule*

undo packet-filter inbound *acl-rule*

View

QoS profile view

Parameters

inbound: Filters the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15.

Description

Use the **packet-filter** command to add the packet filtering action to a QoS profile.

Use the **undo packet-filter** command to remove the packet filtering action from a QoS profile.

Refer to the *ACL* module for the detailed information about packet filtering.

Examples

Add the packet filtering action to QoS profile **a123** to filter the incoming packets matching ACL 4000. (For how to create and configure a Layer 2 ACL, refer to the *ACL* module of this manual.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos-profile a123
[Sysname-qos-profile-a123] packet-filter inbound link-group 4000
```

qos-profile

Syntax

qos-profile *profile-name*

undo qos-profile *profile-name*

View

System view

Parameters

profile-name: QoS profile name, a string of 1 to 32 characters and starting with English letters [a-z, A-Z]. Note that a QoS profile name cannot be **all**, **interface**, **user**, **undo**, or **name**.

Description

Use the **qos-profile** command to create a QoS profile and enter QoS profile view. If the QoS profile already exists, this command leads you to the corresponding QoS profile view.

Use the **undo qos-profile** command to remove a QoS profile.

A QoS profile currently applied to a port cannot be removed.

Examples

Create a QoS profile named **a123**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos-profile a123
[Sysname-qos-profile-a123]
```

qos-profile port-based

Syntax

qos-profile port-based

undo qos-profile port-based

View

Ethernet port view

Parameters

None

Description

Use the **qos-profile port-based** command to configure the QoS profile application mode on a port to be port-based.

Use the **undo qos-profile port-based** command to restore the default.

By default, the application mode of a QoS profile is user-based.

Note that:

- If the 802.1x authentication is MAC-based, you need to configure the QoS profile application mode to be user-based.
- If the 802.1x authentication is port-based, you need to configure the QoS profile application mode to be port-based.

Examples

Configure the QoS profile application mode on GigabitEthernet 1/0/1 to be port-based.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos-profile port-based
```

traffic-limit

Syntax

traffic-limit inbound *acl-rule target-rate* [**conform** *con-action*] [**exceed** *exceed-action*] [**meter-statistic**]

undo traffic-limit inbound *acl-rule* [**meter-statistic**]

View

QoS profile view

Parameters

inbound: Performs traffic policing on the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

target-rate: Rate limit (in kbps) of traffic policing. This argument is in the range 1 to 10000000.

conform *con-action*: Sets the actions of the switch on the packets except forwarding when the packet traffic is within the specified traffic. The *con-action* argument can be:

- **remark-dscp** *dscp-value*: Sets the DSCP value for the packets. The *dscp-value* argument is in the range 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value* : Sets the 802.1p precedence of the packets. The *cos-value* argument is in the range 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

exceed *exceed-action*: Sets the actions on the part of the packets exceeding the specified traffic when the packet traffic exceeds the specified traffic. The actions include:

- **drop**: Drops the packets.
- **forward**: Forwards the packets.
- **remark-dscp** *dscp-value*: Resets the DSCP value for the packets and forwards them at the same time. The *dscp-value* argument is in the range 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.
- **remark-cos** *cos-value*: Resets the 802.1p precedence for the packets and forwards them at the same time. The *cos-value* argument is in the range 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

meter-statistic: Performs the statistics function specific to traffic policing. It can meter the bytes of the packets within the limited rate and the bytes of the packets beyond the limited rate.

Description

Use the **traffic-limit** command to add the traffic policing action to a QoS profile.

Use the **undo traffic-limit** command to remove the traffic policing action from a QoS profile.

The traffic policing action of a QoS profile currently applied to a port cannot be removed.

Examples

Add traffic policing action to the QoS profile named “a123” to limit the rate of the incoming packets matching ACL 2000 to 128 kbps and drop the packets exceeding 128 kbps. (For how to create and configure a basic ACL, refer to the ACL module of this manual.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos-profile a123
[Sysname-qos-profile-a123] traffic-limit inbound  ip-group 2000 128 exceed drop
```

traffic-priority

Syntax

traffic-priority inbound *acl-rule* { **dscp** *dscp-value* | **cos** *cos-value* }

undo traffic-priority inbound *acl-rule*

View

QoS profile view

Parameters

inbound: Performs priority marking on the incoming packets.

acl-rule: ACL rules to be used for traffic classification. The *acl-rule* argument can be a combination of multiple types of ACLs. For more information about the *acl-rule* argument, refer to Table 1-14 and Table 1-15. Note that the ACL rules referenced must be configured with the **permit** keyword.

dscp *dscp-value*: Sets the DSCP value. The *dscp-value* argument is in the range 0 to 63. You can also enter a keyword listed in Table 1-17 for this argument.

cos *cos-value*: Sets the 802.1p precedence value. The *cos-value* argument is in the range 0 to 7. You can also enter a keyword listed in Table 1-32 for this argument.

Description

Use the **traffic-priority** command to add a priority marking action to a QoS profile.

Use the **undo traffic-priority** command to remove a priority marking action from a QoS profile.

The priority marking action of a QoS profile currently applied to a port cannot be removed.

Examples

Add the priority marking action to the QoS profile named **a123** to set the 802.1p precedence value of the incoming packets matching ACL 4000 to 1. (For how to create and configure a Layer 2 ACL, refer to the ACL module of this manual.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] qos-profile a123
[Sysname-qos-profile-a123] traffic-priority inbound link-group 4000 cos 1
```

Table of Contents

1 Mirroring Commands

Mirroring Commands

display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View

Any view

Parameters

group-id: Specifies the mirroring group of which the configurations are to be displayed. The argument takes a value in the range of 1 to 20.

all: Specifies to display the parameter settings of all mirroring groups.

local: Specifies to display the parameter settings of local port mirroring groups.

remote-destination: Specifies to display the parameter settings of the destination groups for remote mirroring.

remote-source: Specifies to display the parameter settings of the source groups for remote mirroring.

Description

Use the **display mirroring-group** command to display port mirroring configurations.

Related commands: **mirroring-group mirroring-port**, **mirroring-group monitor-port**.

Examples

Display the configurations of a local mirroring group on your Switch 4200G series.

```
<Sysname> display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
    mirroring mac:
    mirroring vlan:
    monitor port: GigabitEthernet1/0/2
```

Display the configurations of a remote source mirroring group on your Switch 4200G series.

```
<Sysname> display mirroring-group 2
mirroring-group 2:
    type: remote-source
    status: active
```

```
    mirroring port:
        GigabitEthernet1/0/1  inbound
    mirroring mac:
    mirroring vlan:
    reflector port: GigabitEthernet1/0/2
    remote-probe vlan: 10
```

Display the configurations of a remote destination mirroring group on your Switch 4200G series.

```
<Sysname> display mirroring-group 3
mirroring-group 3:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/3
    remote-probe vlan: 20
```

Table 1-1 Description on the fields of the **display mirroring-group** command

Field	Description
mirroring-group	Port mirroring group number.
type	Port mirroring group type, which can be local, remote-source, or remote-destination.
status	Status of the port mirroring group, which can be active or inactive.
mirroring port	Source port in port mirroring. This field is available only for local mirroring groups or remote source mirroring groups.
both/inbound/outbound	The direction of the mirrored packets, which can be one of the following: • both: means packets received on and sent from the mirroring port are mirrored. • Inbound: means packets received on the mirroring port are mirrored. • outbound: means packets sent from the mirroring port are mirrored.
mirroring mac	The specified MAC address and VLAN ID for MAC-based mirroring
mirroring vlan	The specified VLAN ID for VLAN-based mirroring
monitor port	Destination port. This field is available only for local mirroring groups and remote destination mirroring groups.
reflector port	Reflector port. This field is available only for remote source mirroring groups.
remote-probe vlan	Remote probe VLAN. This field is available only for remote source/destination mirroring groups.

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

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

all: Specifies to remove all mirroring groups.

local: Specifies the mirroring group as a local port mirroring group.

remote-destination: Specifies the mirroring group as the destination mirroring group for remote port mirroring.

remote-source: Specifies the mirroring group as the source mirroring group for remote port mirroring.

Description

Use the **mirroring-group** command to create a port mirroring group.

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

The mirroring group you created can take effect only after you configure other parameters for it.

Note that, a Switch 4200G supports configuring only one destination port in local port mirroring or one reflector port in remote port mirroring. That is, on a Switch 4200G, there can be only one effective local mirroring group or one effective remote source mirroring group. The two mirroring groups cannot coexist.

Related commands: **display mirroring-group**.

Examples

Create a port mirroring group on the local switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-mac

Syntax

mirroring-group *group-id* **mirroring-mac** *mac* **vlan** *vlan-id*

undo mirroring-group *group-id* **mirroring-mac** [[*mac*] **vlan** *vlan-id*]

View

System view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

mac: Specified MAC address, in the format of H-H-H. The MAC address must be a static one existing in the MAC address table.

vlan *vlan-id*: Specifies the VLAN to which the static MAC address belongs.

Description

Use the **mirroring-group mirroring-mac** command to configure the MAC-based mirroring for a local or remote source mirroring group.

Use the **undo mirroring-group mirroring-mac** command to remove the configuration.

Examples

Configure MAC-based mirroring to mirror packets whose source/destination MAC addresses match 000f-e20f-0101 to port GigabitEthernet 1/0/2 on the local device.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-address static 000f-e20f-0101 interface Gigabitethernet 1/0/1 vlan 2
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-mac 000f-e20f-0101 vlan 2
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

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*

View

System view, Ethernet port view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

mirroring-port *mirroring-port-list*: Specifies a list of source ports. *mirroring-port-list* is available in system view only, and there is no such argument in Ethernet port view. *mirroring-port-list* is provided in the format of *mirroring-port-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where *interface-type* is the port type, and *interface-number* is the port number, and &<1-8> means that you can specify up to 8 ports or port lists.

both: Specifies to mirror the packets received on and sent from the source mirroring port.

inbound: Specifies to mirror the packets received on the source mirroring port.

outbound: Specifies to mirror the packets sent from the source mirroring port.

Description

Use the **mirroring-group mirroring-port** command to configure the source ports for a local mirroring group or a remote source mirroring group.

Use the **undo mirroring-group mirroring-port** command to remove the source ports of a local mirroring group or a remote source mirroring group.

Note that:

- You cannot configure a member port of an existing mirroring group as a source port for port mirroring.
- Before configuring a mirroring source port, make sure that the corresponding mirroring group has already been created.

- A copy of each packet passing through a source port will be sent to the corresponding destination port.

Related commands: **display mirroring-group**.

Examples

Configure GigabitEthernet 1/0/1 as the source port of local mirroring group 1, and mirror all packets received on this port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 inbound
```

mirroring-group mirroring-vlan

Syntax

mirroring-group *group-id* **mirroring-vlan** *vlan-id* **inbound**

undo mirroring-group *group-id* **mirroring-vlan** [*vlan-id* **inbound**]

View

System view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

mirroring-vlan *vlan-id*: Specifies a VLAN. The *vlan-id* argument ranges from 1 to 4094. The specified VLAN must be an existing VLAN on the device.

inbound: Specifies to mirror packets received on all ports of the VLAN.

Description

Use the **mirroring-group mirroring-vlan** command to configure the VLAN-based mirroring for a local or remote source mirroring group.

Use the **undo mirroring-group mirroring-vlan** command to remove the configuration.

You can monitor packets of multiple VLANs by executing the **mirroring-group mirroring-vlan** command for several times.

Examples

Configure VLAN-based mirroring to mirror packets received on all ports in VLAN 2 to port GigabitEthernet 1/0/2 on the local device.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-vlan 2 inbound
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

mirroring-group monitor-port

Syntax

mirroring-group *group-id* **monitor-port** *monitor-port*

undo mirroring-group *group-id* **monitor-port** *monitor-port*

View

System view, Ethernet port view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

monitor-port *monitor-port*: Specifies the destination port for port mirroring. *monitor-port* is available in system view only, and there is no such argument in Ethernet port view.

Description

Use the **mirroring-group monitor-port** command to configure the destination port for a local mirroring group or a remote destination mirroring group.

Use the **undo mirroring-group monitor-port** to remove the destination port of a local mirroring group or a remote destination mirroring group.

Note that:

- You cannot configure a member port of an existing mirroring group, a member port of an aggregation group, or a port enabled with LACP or STP as the destination port.
- Before configuring a destination port for a local mirroring group, make sure that the corresponding mirroring group has already been created.
- It is recommended that you use a destination port for port mirroring purpose only. Do not use a destination port to transmit other service packets.

Related commands: **display mirroring-group**.

Examples

Configure GigabitEthernet 1/0/4 as the destination port of local mirroring group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/4
```

mirroring-group reflector-port

Syntax

mirroring-group *group-id* **reflector-port** *reflector-port*

undo mirroring-group *group-id* **reflector-port** *reflector-port*

View

System view, Ethernet port view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

reflector-port *reflector-port*: Specifies the reflector port. *reflector-port* is available in system view only, and there is no such argument in Ethernet port view.

Description

Use the **mirroring-group reflector-port** command to specify the reflector port for a remote source mirroring group.

Use the **undo mirroring-group reflector-port** command to remove the reflector port of a remote source mirroring group.

Note the following when you configure the reflector port:

- The reflector port cannot be a member port of an existing mirroring group, a member port of an aggregation group, or a port enabled with LACP or STP. It must be an access port and cannot be configured with functions like VLAN-VPN, port loopback detection, port security, and so on.
- It is recommended that you use a reflector port for port mirroring purpose only.

Examples

Configure GigabitEthernet 1/0/2 as the reflector port of remote source mirroring group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 reflector-port GigabitEthernet 1/0/2
```

mirroring-group remote-probe vlan

Syntax

mirroring-group *group-id* **remote-probe vlan** *remote-probe-vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *remote-probe-vlan-id*

View

System view

Parameters

group-id: Number of a port mirroring group, in the range 1 to 20.

remote-probe vlan *remote-probe-vlan-id*: Specifies the remote-probe VLAN for the mirroring group.

Description

Use the **mirroring-group remote-probe vlan** command to specify the remote-probe VLAN for a remote source/destination mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the configuration of remote-probe VLAN for a remote source/destination mirroring group.

Note that, before configuring a VLAN as the remote-probe VLAN for a remote source/destination mirroring group, you need to use the **remote-probe vlan enable** command to configure the VLAN as a remote-probe VLAN first.

Related commands: **display mirroring-group**, **remote-probe vlan enable**.

Examples

Configure VLAN 100 as the remote-probe VLAN of remote source mirroring group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 100
[Sysname-vlan100] remote-probe vlan enable
[Sysname-vlan100] quit
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 100
```

mirroring-port

Syntax

mirroring-port { **both** | **inbound** | **outbound** }

undo mirroring-port

View

Ethernet port view

Parameters

both: Specifies to mirror all packets received on and sent from the port.

inbound: Specifies to mirror the packets received on the port.

outbound: Specifies to mirror the packets sent from the port.

Description

Use the **mirroring-port** command to configure the source port in Ethernet port view.

Use the **undo mirroring-port** command to remove the configuration of the source port in Ethernet port view.

Note that:

You cannot configure a member port of an existing mirroring group as a source port for port mirroring.

Related commands: **display mirroring-group**.

 **Note**

When you configure mirroring source port on an Ethernet port of a Switch 4200G, if mirroring group 1 does not exist, the switch will automatically create local mirroring group 1 and add the source port to the group; if mirroring group 1 already exists, but is not a local mirroring group, your configuration of the source port will fail.

Examples

In Ethernet port view, configure GigabitEthernet 1/0/1 as the source port, and mirror all packets received on and sent from this port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-port both
```

monitor-port

Syntax

monitor-port

undo monitor-port

View

Ethernet port view

Parameters

None

Description

Use the **monitor-port** command to configure the destination port in Ethernet port view.

Use the **undo monitor-port** command to remove the configuration of the destination port in Ethernet port view.

Note that:

- You cannot configure a member port of an aggregation group, a member port of an aggregation group, or a port enabled with LACP and STP as the mirroring destination port.
- It is recommended that you use a destination port for port mirroring purpose only. Do not use a destination port to transmit other service packets.

Related commands: **display mirroring-group**.

 **Note**

When you configure mirroring destination port on an Ethernet port of a Switch 4200G, if mirroring group 1 does not exist, the switch will automatically create local mirroring group 1 and add the destination port to the group; if mirroring group 1 already exists, but is not a local mirroring group, your configuration of the destination port will fail.

Examples

Configure GigabitEthernet 1/0/4 as a destination port in Ethernet port view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] monitor-port
```

remote-probe vlan enable

Syntax

remote-probe vlan enable

undo remote-probe vlan enable

View

VLAN view

Parameters

None

Description

Use the **remote-probe vlan enable** command to configure the current VLAN as the remote-probe VLAN.

Use the **undo remote-probe vlan enable** command to restore the remote-probe VLAN to a normal VLAN.

Note that:

- You cannot configure a default VLAN, a management VLAN, or a dynamic VLAN as the remote-probe VLAN.
- A remote-probe VLAN cannot be removed directly. To do that, you need to run the **undo remote-probe vlan enable** command in VLAN view first.

Related commands: **mirroring-group remote-probe vlan**.

Examples

Configure VLAN 5 as the remote-probe VLAN.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 5
[Sysname-vlan5] remote-probe vlan enable
```

Table of Contents

1 ARP Configuration Commands

ARP Configuration Commands

arp check enable

Syntax

arp check enable

undo arp check enable

View

System view

Parameters

None

Description

Use the **arp check enable** command to enable the ARP entry checking function on a switch.

Use the **undo arp check enable** command to disable the ARP entry checking function.

With the ARP entry checking function enabled, the switch cannot learn any ARP entry with a multicast MAC address. Configuring such a static ARP entry is not allowed either; otherwise, the system prompts error information.

After the ARP entry checking function is disabled, the switch can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the switch.

By default, the ARP entry checking function is enabled.

Examples

Disable the ARP entry checking function.

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

arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

arp static *ip-address mac-address vlan-id* (in Ethernet port view)

undo arp *ip-address*

View

System view, Ethernet port view

Parameters

ip-address: IP address contained in the ARP mapping entry to be created/removed.

mac-address: MAC address contained in the ARP mapping entry to be created, in the format of H-H-H.

vlan-id: ID of the VLAN to which the static ARP entry belongs, in the range of 1 to 4,094.

interface-type: Type of the port to which the static ARP entry belongs.

interface-number: Number of the port to which the static ARP entry belongs.

Description

Use the **arp static** command to create a static ARP entry.

Use the **undo arp** command to remove an ARP entry.

By default, the system ARP mapping table is empty and the address mapping entries are obtained by ARP dynamically.

Note that:

- Static ARP entries are valid as long as the Ethernet switch operates normally. But some operations, such as removing a VLAN, or removing a port from a VLAN, will make the corresponding ARP entries invalid and therefore removed automatically.
- As for the **arp static** command, the value of the *vlan-id* argument must be the ID of an existing VLAN, and the port identified by the *interface-type* and *interface-number* arguments must belong to the VLAN.
- Currently, static ARP entries cannot be configured on the ports of an aggregation group.

Related commands: **reset arp**, **display arp**.

Examples

Create a static ARP mapping entry, with the IP address of 202.38.10.2, the MAC address of 000f-e20f-0000. The ARP mapping entry belongs to GigabitEthernet 1/0/1 which belongs to VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] arp static 202.38.10.2 000f-e20f-0000 1 GigabitEthernet 1/0/1
```

arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Parameters

aging-time: Aging time (in minutes) of the dynamic ARP entries. This argument ranges from 1 to 1,440.

Description

Use the **arp timer aging** command to configure the aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

Examples

Configure the aging time to be 10 minutes for dynamic ARP entries.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] arp timer aging 10
```

display arp

Syntax

display arp [**dynamic** | **static** | *ip-address*]

View

Any view

Parameters

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

ip-address: IP address. ARP entries containing the IP address are to be displayed.

Description

Use the **display arp** command to display specific ARP entries.

If you execute this command with no keyword/argument specified, all the ARP entries are displayed.

Related commands: **arp static**, **reset arp**.

Examples

Display all the ARP entries.

```
<Sysname> display arp
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name / AL ID      Aging Type
10.2.72.162      000a-000a-0aaa  N/A      N/A                    N/A   S
192.168.0.77     0000-e8f5-6a4a  1        GigabitEthernet1/0/2    13    D
192.168.0.2      000d-88f8-4e88  1        GigabitEthernet1/0/2    14    D
192.168.0.200    0014-222c-9d6a  1        GigabitEthernet1/0/2    14    D
192.168.0.45     000d-88f6-44c1  1        GigabitEthernet1/0/2    15    D
192.168.0.110    0011-4301-991e  1        GigabitEthernet1/0/2    15    D
192.168.0.32     0000-e8f5-73ee  1        GigabitEthernet1/0/2    16    D
192.168.0.3      0014-222c-aa69  1        GigabitEthernet1/0/2    16    D
192.168.0.17     000d-88f6-379c  1        GigabitEthernet1/0/2    17    D
192.168.0.115    000d-88f7-9f7d  1        GigabitEthernet1/0/2    18    D
192.168.0.43     000c-760a-172d  1        GigabitEthernet1/0/2    18    D
192.168.0.33     000d-88f6-44ba  1        GigabitEthernet1/0/2    20    D
192.168.0.35     000f-e20f-2181  1        GigabitEthernet1/0/2    20    D
192.168.0.5      000f-3d80-2b38  1        GigabitEthernet1/0/2    20    D
```

```
---   14 entries found   ---
```

Table 1-1 Description on the fields of the **display arp** command

Field	Description
IP Address	IP address contained in an ARP entry
MAC Address	MAC address contained in an ARP entry
VLAN ID	ID of the VLAN which an ARP entry corresponds to
Port Name / AL ID	Port which an ARP entry corresponds to
Aging	Aging time (in minutes) of an ARP entry N/A is displayed for static ARP entries.
Type	Type of an ARP entry: D for dynamic, and S for static.

display arp |

Syntax

display arp [**dynamic** | **static**] **|** { **begin** | **exclude** | **include** } *regular-expression*

View

Any view

Parameters

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Configuration File Management Command* in this manual.

begin: Displays the first ARP entry containing the specified string and all subsequent ARP entries.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries containing the specified string.

regular-expression: A case-sensitive character string.

Description

Use the **display arp |** command to display the ARP entries related to string in a specified way.

Related commands: **arp static**, **reset arp**.

Examples

Display all the ARP entries that contain the string **77**.

```
<Sysname> display arp | include 77
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name / AL ID      Aging Type
192.168.0.77     0000-e8f5-6a4a  1        GigabitEthernet1/0/2      12    D

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

Display all the ARP entries that do not contain the string **68**.

```
<Sysname> display arp | exclude 68
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name / AL ID      Aging Type
10.2.72.162      000a-000a-0aaa  N/A      N/A                    N/A   S

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

Refer to Table 1-1 for the description on the above output information.

display arp count

Syntax

display arp count [[**dynamic** | **static**] [**|** { **begin** | **exclude** | **include** } *regular-expression*] | *ip-address*]

View

Any view

Parameters

dynamic: Counts the dynamic ARP entries.

static: Counts the static ARP entries.

|: Uses a regular expression as the match criterion. For detailed information about regular expressions, refer to *Configuration File Management Command* in this manual.

begin: Displays the number of ARP entries counted from the first one containing the specified string.

exclude: Displays the number of ARP entries that do not contain the specified string.

include: Displays the number of ARP entries containing the specified string.

regular-expression: A case-sensitive character string.

ip-address: IP address. The ARP entries containing the IP address are to be displayed.

Description

Use the **display arp count** command to display the number of the specified ARP entries. If no parameter is specified, the total number of ARP entries is displayed.

Related commands: **arp static**, **reset arp**.

Examples

Display the total number of ARP entries.

```
<Sysname> display arp count
 14 entries found
```

display arp timer aging

Syntax

display arp timer aging

View

Any view

Parameters

None

Description

Use the **display arp timer aging** command to display the setting of the ARP aging time.

Related commands: **arp timer aging**.

Examples

Display the setting of the ARP aging time.

```
<Sysname> display arp timer aging
 Current ARP aging time is 20 minute(s)(default)
```

The displayed information shows that the ARP aging time is set to 20 minutes.

gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

View

System view

Parameters

None

Description

Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function. Then, a switch receiving a gratuitous ARP packet can add the IP and MAC addresses carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry for the ARP packet in the cache.

Use the **undo gratuitous-arp-learning enable** command to disable the gratuitous ARP packet learning function.

By default, the gratuitous ARP packet learning function is enabled.

Examples

Enable the gratuitous ARP packet learning function on a switch.

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

reset arp

Syntax

reset arp [**dynamic** | **static** | **interface** *interface-type interface-number*]

View

User view

Parameters

dynamic: Clears dynamic ARP entries.

static: Clears static ARP entries.

interface *interface-type interface-number*: Clears ARP entries of the specified port.

Description

Use the **reset arp** command to clear specific ARP entries.

Related commands: **arp static**, **display arp**.

Examples

Clear static ARP entries.

```
<Sysname> reset arp static
```

2 ARP Attack Defense Configuration Commands

ARP Attack Defense 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

Parameters

None

Description

Use the **arp anti-attack valid-check enable** command to enable ARP source MAC address consistency check.

Use the **undo arp anti-attack valid-check enable** command to disable this function.

By default, ARP source MAC address consistency check is disabled.

Examples

Enable ARP source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

arp detection enable

Syntax

arp detection enable

undo arp detection enable

View

VLAN view

Parameters

None

Description

Use the **arp detection enable** command to enable the ARP attack detection function on all ports in the specified VLAN. When receiving an ARP packet from a port in this VLAN, the switch will check the

source IP address, source MAC address, number of the receiving port, and the VLAN of the port. If the mapping of the source IP address and source MAC address is not included in the DHCP snooping entries or IP static binding entries, or the number of the receiving port and the VLAN of the port do not match the DHCP snooping entries or IP static binding entries, the ARP packet will be discarded.

Use the **undo arp detection enable** command to disable the ARP attack detection function on all ports in the specified VLAN.

By default, ARP attack detection is disabled on the switch.

Examples

Enable ARP attack detection on all ports in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 1
[Sysname-vlan1] arp detection enable
```

arp detection trust

Syntax

arp detection trust

undo arp detection trust

View

Ethernet port view

Parameters

None

Description

Use the **arp detection trust** command to specify the current port as a trusted port, that is, ARP packets received on this port are regarded as legal ARP packets and will not be checked.

Use the **undo arp detection trust** command to specify the current port as an untrusted port in ARP detection.

By default, a port is an untrusted port in ARP detection.

Examples

Specify GigabitEthernet 1/0/11 as the trusted port in ARP detection.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] arp detection trust
```

arp filter source

Syntax

arp filter source *ip-address*

undo arp filter source

View

Ethernet port view

Parameters

ip-address: IP address of the gateway.

Description

Use the **arp filter source** command to configure ARP packet filtering based on the gateway's IP address on the current port working as the downstream port connected to a host. After that, ARP packets from the host with the gateway's IP address as the sender IP address are considered invalid and discarded.

Use the **undo arp filter source** command to remove the configuration.

By default, ARP packet filtering based on the gateway's IP address is disabled.

Note that:

- This command should be configured on a port directly connected to hosts.
- If you execute this command repeatedly, the last configured command takes effect.

Examples

Configure ARP packet filtering based on the gateway's IP address 192.168.0.1/24 on GigabitEthernet 1/0/1.

<Sysname> system-view

```
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 192.168.0.1
```

arp filter binding

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding

View

Ethernet port view

Parameters

ip-address: IP address of the gateway.

mac-address: MAC address of the gateway.

Description

Use the **arp filter binding** command to configure ARP packet filtering based on the gateway's IP and MAC addresses on the current port. After that, the port will discard ARP packets with the gateway's IP address as the sender IP address but with the sender MAC address different from that of the gateway.

Use the **undo arp filter binding** command to remove the configuration.

By default, ARP packet filtering based on the gateway's IP and MAC addresses are disabled.

Note that:

- This command should be configured on a cascaded port or upstream port of an access switch.
- If you execute this command repeatedly, the last configured command takes effect.

Examples

Configure ARP packet filtering based on the gateway's IP address 192.168.100.1/24 and MAC address 000d-88f8-528c on GigabitEthernet 1/0/2.

<Sysname> system-view

```
[Sysname] interface gigabitethernet1/0/2
[Sysname-GigabitEthernet1/0/2] arp filter binding 192.168.100.1 000d-88f8-528c
```

arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

View

VLAN interface view

Parameters

number: Maximum number of dynamic ARP entries that can be learned by the interface. The effective range is 1 to 256.

Description

Use the **arp max-learning-num** command to configure the maximum number of dynamic ARP entries that can be learned by the current VLAN interface.

Use the **undo arp max-learning-num** command to remove the configuration.

By default, the maximum number of dynamic ARP entries that can be learned by a VLAN interface is 256.

If you execute this command repeatedly, the last configured command takes effect.

Examples

Configure the maximum number of dynamic ARP entries that can be learned by VLAN-interface 40 as 500.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 500
```

arp protective-down recover enable

Syntax

arp protective-down recover enable

undo arp protective-down recover enable

View

System view

Parameters

None

Description

Use the **arp protective-down recover enable** command to enable the port state auto-recovery function on the switch.

Use the **undo arp protective-down recover enable** command to disable the port state auto-recovery function of a switch.

With this function enabled, the switch can automatically bring up a port that has been shut down due to an excessive ARP packet receiving rate after a specified period.

By default, the port state auto-recovery function is disabled.

Examples

Enable the port state auto-recovery function of the switch.

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

arp protective-down recover interval

Syntax

arp protective-down recover interval *interval*

undo arp protective-down recover *interval*

View

System view

Parameters

interval: Recovery time (in seconds) of a port which is shut down due to an excessive ARP packet receiving rate. The effective range is 10 to 86,400.

Description

Use the **arp protective-down recover interval** command to specify a recovery interval. After the interval, a port that has been shut down due to an excessive ARP packet receiving rate will be brought up.

Use the **undo arp protective-down recover interval** command to restore the default.

By default, when the port state auto-recovery function is enabled, the recovery interval is 300 seconds.

Note that:

- You need to enable the port state auto-recovery feature before you can configure the auto-recovery interval.
- If you use the **arp protective-down recover interval** command to modify the recovery time when the current port has been already shut down due to an excessive ARP packet receiving rate, the previously configured interval applies to the first port state recovery. Starting from the next state recovery, the new recovery interval will take effect.

Examples

Set the auto-recovery interval to 30 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] arp protective-down recover enable
[Sysname] arp protective-down recover interval 30
```

arp rate-limit

Syntax

arp rate-limit *rate*

undo arp rate-limit

View

Ethernet port view

Parameters

rate: Maximum ARP packet receiving rate on the port, in the range of 10 to 1,024 pps.

Description

Use the **arp rate-limit** command to specify the maximum ARP packet receiving rate on the port. If a rate is specified, exceeding packets will be discarded.

Use the **undo arp rate-limit** command to restore the default.

By default, after a port is enabled with the ARP packet rate limit function, the maximum ARP packet receiving rate on the port is 15 pps.

Note that:

You must enable the ARP packet rate limit function before you can specify the maximum ARP packet receiving rate on the port by using the **arp rate-limit** command.

Examples

Set the maximum ARP packet receiving rate on GigabitEthernet 1/0/11 to 100 pps.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] arp rate-limit enable
[Sysname-GigabitEthernet1/0/11] arp rate-limit 100
```

arp rate-limit enable

Syntax

arp rate-limit enable

undo arp rate-limit enable

View

Ethernet port view

Parameters

None

Description

Use the **arp rate-limit enable** command to enable the ARP packet rate limit function on the port, that is, to limit the rate of ARP packets passing through the port. If a rate (the maximum ARP packet rate is 15 pps by default) is specified, exceeding ARP packets will be discarded.

Use the **undo arp rate-limit enable** command to disable the ARP packet rate limit function on the port.

By default, the ARP packet rate limit function is disabled, that is, ARP packet rate is not limited on a port.

Examples

Enable the ARP packet rate limit function on GigabitEthernet 1/0/11.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] arp rate-limit enable
```

arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

View

VLAN view

Parameters

None

Description

Use the **arp restricted-forwarding enable** command to enable ARP restricted forwarding so that the legal ARP requests received from the specified VLAN are forwarded through configured trusted ports only, and the legal ARP responses are forwarded according to the MAC addresses in the packets, or through trusted ports if the MAC address table contains no such destination MAC addresses.

Use the **undo arp restricted-forwarding enable** command to disable ARP restricted forwarding.

By default, ARP restricted forwarding is disabled.

Related commands: **arp detection enable**, **arp detection trust**

Syntax

Enable ARP restricted forwarding in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 1
[Sysname-vlan1] arp restricted-forwarding enable
```

display arp detection statistics interface

Syntax

display arp detection statistics interface *interface-type interface-number*

View

Any view

Parameters

interface-type interface-number: Type and number of a port.

Description

Use the **display arp detection statistics interface** command to display the statistics of ARP attack detection state, ARP trusted port state, and discarded invalid ARP packets (those failed to pass ARP attack detection) on the specified port.

If ARP attack detection is disabled, the statistics of ARP trusted port state and discarded invalid ARP packets will not be displayed.

Examples

Display ARP detection statistics on GigabitEthernet 1/0/10.

```
<Sysname> display arp detection statistics interface gigabitethernet1/0/10
 ARP DETECTION : ENABLE
 ARP PORT TRUST : DISABLE
 INVALID ARP PACKETS  : 31
```

Table 2-1 Description on the fields of the **display arp detection statistics interface** command

Field	Description
ARP DETECTION	ARP attack detection state: enabled/disabled
ARP PORT TRUST	ARP trusted port state: enabled/disabled
INVALID ARP PACKETS	Number of discarded invalid ARP packets (those failed to pass ARP attack detection)

ip source static import dot1x

Syntax

ip source static import dot1x

undo ip source static import dot1x

View

System view

Parameters

None

Description

Use the **ip source static import dot1x** command to enable ARP attack detection based on IP-to-MAC mappings of authenticated 802.1x clients. Enabled with this function, switch records mappings between IP addresses (both static and dynamic IP addresses) and MAC addresses of authenticated 802.1x clients and uses the mappings for ARP attack detection after IP-to-MAC static bindings and DHCP snooping entries are checked.

Use the **undo ip source static import dot1x** command to disable the function.

By default, this function is disabled.

Note that this command should be used in cooperation with the **arp detection enable** command.

Examples

Enable the switch to record IP-to-MAC bindings of authenticated 802.1x clients.

```
<Sysname> system-view
[Sysname] ip source static import dot1x
```

Table of Contents

1 Stack Function Configuration Commands

Note

Among Switch 4200G series switches, Switch 4200G 24-Port, Switch 4200G PWR 24-Port, and Switch 4200G 48-Port switches support stacks formed by 10GE stack boards.

Stack Function Configuration Commands

display stacking

Syntax

display stacking [**members**]

View

Any view

Parameter

members: Displays the information about the members of a stack. Do not specify this keyword when you execute this command on a slave switch.

Description

Use the **display stacking** command to display the information about the main switch or the slave switches of a stack.

When you execute this command on a main switch, the information displayed depends on the **members** keyword as follows:

- If the **members** keyword is not specified, the output information indicates that the local switch is the main switch. Besides, the number of the switches contained in the stack is also displayed.
- If the **members** keyword is specified, the information about the members of the stack is displayed, including the stack numbers of the main/slave switches, stack name, stack device name, MAC address and status.

When you execute this command on a slave switch, the information displayed indicates that the local switch is a slave switch. Besides, the information such as the stack number of the local switch, and the MAC address of the main switch in the stack is also displayed.

Example

Display the information about a stack on the main switch.

```
<stack_0.Sysname> display stacking
```

```
Main device for stack.
 Total members:3
 Management-vlan:1(default vlan)
```

Display the information about the stack members on the main switch.

```
<stack_0.Sysname> display stacking members
 Member number: 0
 Name:stack_0.Sysname
 Device: Switch 4200G 12-Port
 MAC Address:000f-e20f-3124
 Member status:Admin
 IP: 129.10.1.15 /16

 Member number: 1
 Name:stack_1.Sysname
 Device: Switch 4200G 24-Port
 MAC Address: 000f-e200-3130
 Member status:Up
 IP: 129.10.1.16/16

Member number: 2
 Name:stack_2.Sysname
 Device: Switch 4200G 12-Port
 MAC Address: 000f-e200-3135
 Member status:Up
 IP: 129.10.1.17/16
```

Table 1-1 Description on the fields of the **display stacking** command

Field	Description
Member number	Numbers of the switches in the stack The main switch is numbered 0.
Name	Name of a slave switch
Device	Device type
MAC Address	Mac address of a switch in the stack
Member status	Status of a switch in the stack “Cmdr” indicates the switch is the main switch; “UP” indicates the switch is on.
IP: 129.10.1.15/16	IP address of a switch in the stack

stacking

Syntax

stacking *number*

View

User view

Parameter

number: Number of the slave switch to switch to.

Description

Use the **stacking** command to switch to a slave switch to configure it.

You can use this command to switch from user view of the main switch to user view of a slave switch. To switch from a slave switch back to the main switch, execute the **quit** command in user view.

 **Note**

Remove the IP address configured for the existing Layer 3 interface first if you want to cancel the stack-related configuration, otherwise, IP address conflicts may occur.

Example

Switch from the main switch to the slave switch numbered 1 and then switch back to the main switch.

```
<stack_0.Sysname> stacking 1
<stack_1.Sysname>
<stack_1.Sysname> quit
<stack_0.Sysname>
```

stacking enable

Syntax

stacking enable

undo stacking enable

View

System view

Parameter

None

Description

Use the **stacking enable** command to create a stack.

Use the **undo stacking enable** command to remove a stack.

The **stacking enable** command triggers a main switch to add the switches connected to its stack ports to the stack.

The **undo stacking enable** command can only be executed on a main switch.

A slave switch quits the stack automatically when it is disconnected from the stack.

Example

Create a stack.

```
<Sysname> system-view
[Sysname] stacking enable
[stack_0.Sysname] quit
<stack_0.Sysname>
```

stacking ip-pool

Syntax

stacking ip-pool *from-ip-address ip-address-number* [*ip-mask*]

undo stacking ip-pool

View

System view

Parameter

from-ip-address: Start address of the stack IP address pool.

ip-address-number: Number of the IP addresses in the stack IP address pool. A stack IP address pool contains 16 addresses by default.

ip-mask: Mask of the stack IP address.

Description

Use the **stacking ip-pool** command to create a stack IP address pool.

Use the **undo stacking ip-pool** command to restore the default stack IP address pool.

You need to create an IP address pool for a stack before creating the stack. When adding a switch to a stack, the main switch picks an IP address from the IP address pool and assigns the IP address to it.

The **stacking ip-pool** command can only be executed on switches that do not belong to any stack. That is, the IP address pool of an existing stack cannot be modified.

To add a switch to a stack successfully, make sure the value of the *ip-address-number* argument is larger than the number of switches currently contained in the stack.

Make sure the IP addresses in the IP address pool of a stack are successive so that they can be assigned successively. For example, the IP addresses in an IP address pool with its start IP address something like 223.255.255.254 are not successive. In this case, errors may occur when adding a switch to the stack.

IP addresses in the IP address pool of a stack must be of the same network segment. For example, the 1.1.255.254 is not a qualified start address for a stack IP address pool.

Note the following when performing stack-related configurations on the main switch of a stack:

- After a stack is created, the main switch automatically adds the switches connected to its stack ports to the stack.
- A slave switch quits the stack automatically when it is disconnected from the stack.
- If the IP address of the management VLAN interface of the main switch (or a slave switch) is not of the same network segment as that of the stack address pool, the main switch (or the slave switch)

automatically removes the existing IP address and picks a new one from the stack address pool as its IP address.

Example

Configure the IP address pool for the stack.

```
<Sysname> system-view
[Sysname] stacking ip-pool 129.10.1.1 5
```

2 Cluster Configuration Commands

NDP Configuration Commands

display ndp

Syntax

display ndp [**interface** *interface-list*]

View

Any view

Parameters

interface *interface-list*: Specifies a port list. You need to provide the *interface-list* argument in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where **to** is used to specify a port range, and &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument. The *interface-number* argument is in the format of unit ID/slot number/port number.

Description

Use the **display ndp** command to display all NDP configuration and operating information, including the global NDP status, the interval to send NDP packets, the holdtime of NDP information, and the NDP status and neighbor information on all ports.

If executed with the **interface** keyword, the **display ndp** command will display the NDP status of the specified interfaces and the related information of the peer device. If executed without the **interface** keyword, the command will display the global NDP configuration information and the statistics on NDP packets received on and sent by each port.

Examples

Display all NDP configuration and operating information.

```
<aaa_0.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: 3044, Pkts Rvd: 3042, Pkts Err: 0
    Neighbor 1:  Aging Time: 161(s)
       MAC Address : 000f-e200-5111
       Host Name   : Sysname
       Port Name   : GigabitEthernet1/0/36
       Software Ver: 3Com OS V3.02.00s56
       Device Name : Switch 4200G 48-Port
```

```
       Port Duplex : AUTO
       Product Ver : 4200G
       BootROM Ver : 2.00
 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
```

……(Omitted)

Display NDP information about GigabitEthernet 1/0/1.

```
<aaa_0.Sysname> display ndp interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
    Status: Enabled, Pkts Snd: 3047, Pkts Rvd: 3045, Pkts Err: 0
    Neighbor 1:  Aging Time: 129(s)
       MAC Address : 000f-e200-5111
       Host Name   : Sysname
       Port Name   : GigabitEthernet1/0/36
       Software Ver: 3Com OS V3.02.00s56
       Device Name : Switch 4200G 48-Port
       Port Duplex : AUTO
       Product Ver : 4200G
       BootROM Ver : 2.00
```

Table 2-1 Description on the fields of the two commands

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the switch.
Neighbor Discovery Protocol Ver: 1	NDP version 1 is running.
Hello Timer	Interval for the switch to send NDP packets, which is configured through the **ndp timer hello** command
Aging Timer	Holdtime for neighbors to keep the NDP information of the switch, which is configured through the **ndp timer aging** command
Interface	Port index, used to identify a port
Status	NDP state on the port (enabled/disabled)
Pkts Snd:	Number of NDP packets sent by the port
Pkts Rvd:	Number of NDP packets received by the port
Pkts Err:	Number of error NDP packets received by the port
Neighbor 1: Aging Time	Holdtime for this switch to keep the NDP information of the neighbor connected to the port
MAC Address	MAC address of the neighbor device

Field	Description
Port name	Port name of the neighbor device
Software Ver	Software version of the neighbor device
Device Name	Device name of the neighbor device
Port Duplex	Port (full/half) duplex mode of the neighbor device
Product Ver	Product version of the neighbor device

ndp enable

Syntax

ndp enable [**interface** *interface-list*]

undo ndp enable [**interface** *interface-list*]

View

System view, Ethernet port view

Parameters

interface-list: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where **to** is used to specify a port range, and &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument. The *interface-number* argument is in the format of unit ID/slot number/port number.

Description

Use the **ndp enable** command to enable NDP globally or on a port.

Use the **undo ndp enable** command to disable NDP globally or on a port.

If you execute the **ndp enable** command in system view without the **interface** keyword specified, NDP will be enabled globally; if you specify the **interface** keyword in the command, NDP will be enabled on the specified ports. In Ethernet port view, the **interface** keyword is unavailable, and execution of the command will enable NDP on the current port only.

By default, NDP is enabled both globally and on ports.

Note that NDP can take effect on a port only when NDP is enabled both globally and on the port.

Examples

Enable NDP globally, and then enable NDP on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ndp enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
```

ndp timer aging

Syntax

ndp timer aging *aging-in-seconds*

undo ndp timer aging

View

System view

Parameters

aging-in-seconds: Holdtime of the NDP information, ranging from 5 to 255 seconds.

Description

Use the **ndp timer aging** command to set the holdtime of the NDP information. This command specifies how long an adjacent device should hold the NDP neighbor information received from the local switch before discarding the information.

Use the **undo timer aging** command to restore the default holdtime of NDP information.

By default, the holdtime of NDP information is 180 seconds.

You can specify how long the adjacent devices should hold the NDP information received from the local switch. When an adjacent device receives an NDP packet from the local switch, it learns how long it should keep the NDP information of the switch according to the holdtime carried in the NDP packet, and discards the NDP information when the holdtime expires.

Note that NDP information holdtime should be longer than the interval between sending NDP packets. Otherwise, a neighbor entry will be generated and age out frequently, resulting in instability of the NDP port neighbor table.

Examples

Set the holdtime of the NDP information sent by the switch to 60 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ndp timer aging 60
```

ndp timer hello

Syntax

ndp timer hello *timer-in-seconds*

undo ndp timer hello

View

System view

Parameters

timer-in-seconds: Interval between sending NDP packets, ranging from 5 to 254 seconds.

Description

Use the **ndp timer hello** command to set the interval between sending NDP packets.

Use the **undo ndp timer hello** command to restore the default interval.

By default, this interval is 60 seconds.

A switch should update the NDP information of its neighbors regularly, so that the switch can get the updated information of the neighbors in time. You can use the **ndp timer hello** command to specify the interval at which the switch sends hello packets to its neighbors for NDP information update.

Note that NDP information holdtime should be longer than the interval between sending NDP packets. Otherwise, a neighbor entry will be generated and age out frequently, resulting in instability of the NDP port neighbor table.

Examples

Set the interval between sending NDP packets to 80 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ndp timer hello 80
```

reset ndp statistics

Syntax

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

View

User view

Parameters

interface-list: Ethernet port list, in the format of { *interface-type interface-number* [**to** i*nterface-type interface-number*] } &<1-10>, where **to** is used to specify a port range, and &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument. The interface-number argument is in the format of unit ID/slot number/port number.

Description

Use the **reset ndp statistics** command to clear the NDP statistics on specific ports. When executing the command, if you specify the **interface** keyword, the command will clear NDP statistics on the specified ports; if you do not specify the **interface** keyword, the command will clear NDP statistics on all ports.

You can use the **display ndp** command to view the NDP statistics before and after the execution of the **reset ndp statistics** command to verify the execution result.

Examples

Display the NDP statistics on port GigabitEthernet 1/0/6.

```
<Sysname>  display ndp interface GigabitEthernet 1/0/6
 Interface: GigabitEthernet1/0/6
    Status: Enabled, Pkts Snd: 1, Pkts Rvd: 2, Pkts Err: 0
```

Clear the NDP statistics on port GigabitEthernet 1/0/6.

```
<Sysname> reset ndp statistics interface GigabitEthernet 1/0/6
```

Re-display the NDP statistics on port GigabitEthernet 1/0/6.

```
<Sysname> display ndp interface GigabitEthernet 1/0/6
 Interface: GigabitEthernet1/0/6
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
```

NTDP Configuration Commands

display ntdp

Syntax

display ntdp

View

Any view

Parameters

None

Description

Use the **display ntdp** command to display the global NTDP information.

The displayed information includes topology collection range (hop count), topology collection interval (NTDP timer), device/port forwarding delay of topology collection requests, and time used by the last topology collection.

Examples

Display the global NTDP information.

```
<Sysname> display ntdp
 NTDP is running.
 Hops      : 4
 Timer     : 0 min(disable)
 Hop Delay : 100 ms
 Port Delay: 10 ms
 Last collection total time: 92ms
```

Table 2-2 Description on the fields of the **display ntdp** command

Field	Description
NTDP is running.	NTDP is enabled globally on this device.
Hops	Hop count for topology collection, which is configured through the **ntdp hop** command
Timer	Interval to collect topology information, which is configured through the **ntdp timer** command "disable" means this switch is not a management device and does not perform periodic topology collection.

Field	Description
Hop Delay	Delay for other devices to forward topology collection requests, which is configured through the **ntdp timer hop-delay** command
Port Delay	Delay for ports on other devices to forward topology collection requests, which is configured through the **ntdp timer port-delay** command
Last collection total time	Time used by the last topology collection

display ntdp device-list

Syntax

display ntdp device-list [**verbose**]

View

Any view

Parameters

verbose: Displays the detailed information of devices in a cluster.

Description

Use the **display ntdp device-list** command to display the cluster device information collected by NTDP.

Examples

Display the list of devices collected by NTDP.

```
<Sysname> display ntdp device-list
MAC               HOP  IP                  PLATFORM
000f-e20f-3901    0    100.100.1.1/24      4200G 12-Port
000f-e20f-3190    1    16.1.1.1/24         4200G 24-Port
```

Table 2-3 Description on the fields of the **display ntdp device-list** command

Field	Description
MAC	MAC address of a device collected by NTDP
HOP	Hops from this device to the collected device
IP	IP address and mask length of the management VLAN interface on the collected device
PLATFORM	Platform information about the collected device

Display detailed device information collected by NTDP.

```
<Sysname> display ntdp device-list verbose

 Hostname   : test_0.4200G
 MAC        : 00e0-fc00-5200
```

```
Hop       : 0
Platform  : 4200G 12-Port
IP        : 192.168.0.91/16
Version   :
  3Com Versatile Routing Platform Software
  Comware Software, Version 3Com OS V3.02.01s168
  Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
  Switch 4200G 12-Port 4200G

Cluster   :  Administrator switch of cluster test
Stack     :  Candidate switch

Peer MAC        Peer Port ID            Native Port ID          Speed Duplex
00e0-fc02-2180  GigabitEthernet1/0/9    GigabitEthernet1/0/5    100   FULL
00e0-fc00-5104  GigabitEthernet1/0/16   GigabitEthernet1/0/2    1000  FULL
```

Table 2-4 Description on the fields of display ntdp device-list verbose

Field	Description
Hostname	System name of a device collected by NTDP
MAC	MAC address of the collected device
Hop	Hops from this device to the collected device
Platform	Software platform of the collected device
IP	IP address and mask length of the cluster management VLAN interface on the collected device
Version	Software version of the collected device
Cluster	The role of the collected device for the cluster
Peer MAC	MAC address of a neighbor device connected to the collected device
Peer Port ID	Index of the port on the neighbor device connected to the collected device
Native Port ID	Index of the port on the collected device connected to the neighbor device
Speed	Speed of the neighbor device port
Duplex	Duplex mode of the neighbor device port

ntdp enable

Syntax

ntdp enable

undo ntdp enable

View

System view, Ethernet port view

Parameters

None

Description

Use the **ntdp enable** command to enable NTDP globally or on a port.

Use the **undo ntdp enable** command to disable NTDP globally or on a port.

By default, NTDP is enabled both globally and on ports.

Note that NTDP can take effect on a port only when NTDP is enabled both globally and on the port.

Examples

Enable NTDP globally, and then enable NTDP on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntdp enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntdp enable
```

ntdp explore

Syntax

ntdp explore

View

User view

Parameters

None

Description

Use the **ntdp explore** command to manually start a topology collection process.

NTDP is able to periodically collect topology information. In addition, you can use this command to manually start a topology collection process at any moment. If you do this, NTDP collects NDP information from all devices in a specific network range (which can be set through the **ntdp hop** command) as well as the connection information of all its neighbors. Through this information, the management device or the network management software knows the topology in the network range, and thus it can manage and monitor the devices in the range.

Examples

Start a topology collection process.

```
<Sysname> ntdp explore
```

ntdp hop

Syntax

ntdp hop *hop-value*

undo ntdp hop

View

System view

Parameters

hop-value: Maximum hops to collect topology information, namely, the topology collection range, in the range of 1 to 16.

Description

Use the **ntdp hop** command to set the topology collection range.

Use the **undo ntdp hop** command to restore the default topology collection range.

By default, the topology collection range is three hops.

With the **ntdp hop** command, you can specify to collect topology information from the devices within a specified range to avoid infinite collection. That is, you can limit the range of topology collection by setting the maximum hops from the collecting device to the collected devices. For example, if you set the maximum hops to two, the switch initiating the topology collection collects topology information from the switches within two hops.

Note that:

- The topology collection range set by this command is applicable to both the periodic and manual topology collection.
- This command is only applicable to topology-collecting device, and a wider collection range requires more memory of the topology-collecting device.

Examples

Set the topology collection range to 5 hops.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] ntdp hop 5
```

ntdp timer

Syntax

ntdp timer *interval-in-minutes*

undo ntdp timer

View

System view

Parameters

interval-in-minutes: Interval (in minutes) to collect topology information, ranging from 0 to 65,535. A value of 0 disables topology information collection.

Description

Use the **ntdp timer** command to configure the interval to collect topology information periodically.

Use the **undo ntdp timer** command to restore the default interval.

By default, this interval is one minute.

After the interval is set to a non-zero value, the switch will collect topology information periodically at this interval. You can also use the **ndp explore** command to start a topology collection process manually.

Note that:

- Only the management switch can collect topology periodically, and a member switch cannot. However, you can use the **ndp explore** command on the member switch to start a topology collection process manually.
- After a cluster is set up, the management switch will collect the topology information of the network at the topology collection interval you set and automatically add the candidate switches it discovers into the cluster.
- If you do not want the candidate switches to be automatically added into the cluster, you can set the topology collection interval to zero, and use the **add-member** command to add the candidate switches to the cluster manually.

Examples

Set the topology collection interval to 30 minutes.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] ntdp timer 30
```

ntdp timer hop-delay

Syntax

ntdp timer hop-delay *time*

undo ntdp timer hop-delay

View

System view

Parameters

time: Device forwarding delay in milliseconds. This argument ranges from 1 to 1,000.

Description

Use the **ntdp timer hop-delay** command to set the delay for devices to forward topology collection requests.

Use the **undo ntdp timer hop-delay** command to restore the default device forwarding delay.

By default, the device forwarding delay is 200 ms.

Network congestion may occur if large amount of topology response packets reach the collecting device in a short period. To avoid this case, each collected switch in the network delays for a period before it forwards a received topology collection request through each NTDP-enabled port.

You can use the **ntdp timer hop-delay** command to set the delay on a collecting switch. The delay value you set by the command is carried in the topology collection requests sent by the collecting switch, and is used by collected devices to determine how long they should wait before they can forward the received topology collection requests.

Examples

Set the delay for collected switches to forward topology collection requests to 300 ms.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] ntdp timer hop-delay 300
```

ntdp timer port-delay

Syntax

ntdp timer port-delay *time*

undo ntdp timer port-delay

View

System view

Parameters

time: Port forwarding delay in milliseconds. This argument ranges from 1 to 100.

Description

Use the **ntdp timer port-delay** command to configure the topology request forwarding delay between two ports, that is, the interval at which the device forwards the topology requests through the NTDP-enabled ports one after another.

Use the **undo ntdp timer port-delay** command to restore the default port forwarding delay.

By default, the port forwarding delay is 20 ms.

Network congestion may occur if large amount of topology response packets reach the collecting device in a short period. To avoid this case, after a collected switch forwards a received topology collection request through a port, it delays for a period before it forwards the request through the next port. You can use the **ntdp timer port-delay** command to set the delay.

You can use the command on a collecting switch. The delay value you set by the **ntdp timer port-delay** command is carried in the topology collection requests sent by the collecting switch, and is used by collected devices to determine the topology collection request forwarding delay between two ports.

Examples

Set the port forwarding delay for collected switches to forward NTDP requests to 40 ms.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] ntdp timer port-delay 40
```

Cluster Configuration Commands

add-member

Syntax

add-member [*member-number*] **mac-address** *H-H-H* [**password** *password*]

View

Cluster view

Parameters

member-number: Member number assigned to the candidate device to be added to the cluster. This argument ranges from 1 to 255.

H-H-H: MAC address of the candidate device to be added (in hexadecimal).

password: Super password of the candidate device, a string of 1 to 256 characters. Password authentication is required when you add a candidate device to a cluster. If the input password is not consistent with the super password configured on the candidate device (through the **super password** command, refer to the *CLI* part of the manual), you cannot add the candidate device to the cluster. If a candidate device is not configured with a super password, you can add it to the cluster without providing the *password* argument).

Description

Use the **add-member** command to add a candidate device to the cluster.

You can only use this command on the management device of a cluster.

If you do not specify the member number when adding a new cluster member, the management device assigns the next available member number to the new member. If you want to specify the member manually, you need to specify a number that is never used by a member device of the cluster.

After you add a candidate device to the cluster, the super password of the device automatically changes to the super password of the management device. If the management device changes its super password, the member devices will automatically synchronize their super passwords to the new super password of the management device.

Examples

Add a candidate device, whose MAC address and user password are 000f-e20f-35e7 and 123456 respectively, to the cluster, and set the member number to 6.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] add-member 6 mac-address 000f-e20f-35e7 password 123456
```

administrator-address

Syntax

administrator-address *mac-address* **name** *name*

undo administrator-address

View

Cluster view

Parameters

mac-address: MAC address of the management device to be specified.

name: Name of an existing cluster, a string of up to 8 characters. Note that the name of a cluster can only contain alphanumeric characters, minus signs (-), and underscores (_).

Description

Use the **administrator-address** command to specify the management device MAC address and the cluster name on a device to add the device to the cluster.

Use the **undo administrator-address** command to remove the management device MAC address from the MAC address list of a member device, that is, remove the member device from the cluster. Normally, this command is used for debugging and restoring purpose.

By default, a switch is not a member of any cluster.

A cluster has one and only one management device. Setting the management device MAC address on a device can add the device to the cluster and enable the device to identify the management device even if it restarts.

You can add a device to a cluster using the **administrator-address** command no matter whether the super password of the device is consistent with that of the management device.

Normally it is recommended to use the **delete-member** command on the management device to remove a member device from the cluster.

Examples

Remove the current member device from the cluster.

```
<aaa_1.Sysname> system-view
System View: return to User View with Ctrl+Z
[aaa_1.Sysname] cluster
[aaa_1.Sysname-cluster] undo administrator-address
```

auto-build

Syntax

auto-build [**recover**]

View

Cluster view

Parameters

recover: Recovers all member devices.

Description

Use the **auto-build** command to start an automatic cluster building process.

You can execute this command on a management device or on a switch to be configured as a management device.

When you execute this command on a candidate device, you are prompted to enter a cluster name to build a cluster. The candidate device will automatically become the management device of the cluster. Then, the management device will collect candidate devices and add them to the cluster automatically.

When you execute this command on a management device, the system directly collects candidate devices and automatically adds them to the cluster.

The **recover** keyword is used to recover a cluster. After you execute the **auto-build recover** command, the system looks for the down members in the member list and add them to the cluster again.

Note that, the collection of candidate/member devices are based on NTDP. Therefore, you must first enable NTDP. In addition, you can use the **ntdp hop** command in system view to change the collection range.

When the system automatically adds a device to the cluster, if the user password configured for the device is different from that of the management device, the device cannot be added to the cluster.

Note

- After a cluster is built automatically, ACL 3998 and ACL 3999 will automatically generate a rule respectively to prohibit packets whose source and destination addresses are private IP addresses of the cluster from being sent to or received from the public network. The two ACL rules will be automatically applied to all ports of the cluster members.
- After a cluster is built automatically, ACL 3998 and ACL 3999 can neither be configured/modified nor removed.

Examples

Start an automatic cluster building process.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] cluster
[Sysname-cluster] auto-build
 There is no base topology, if set up from local flash file?(Y/N)
n

 Please input cluster name:aaa
 Collecting candidate list, please wait...


#Apr  2 07:18:05:357 2000 aaa_0.4200G CLST/5/Cluster_Trap:- 1 -
OID:1.3.6.1.4.1.43.45.1.6.7.1.0.3(hgmpMemberStatusChange):member
00.00.00.00.00.e0.fc.00.51.00  role  change,  NTDPIndex:0.00.00.00.00.00.e0.fc.00.51.00,
Role:1
Candidate list:

 Name                          Hops  MAC Address     Device
 4200G                         2     0016-e0c0-c201  4200G 12-Port
 4200G                         2     000f-e221-616e  4200G 24-Port
 4200G                         2     000f-e202-2180  4200G 12-Port
 SwitchA                       2     0016-e0be-e200  4200G 48-Port
 4500                          3     000f-e200-1774  4500 26-Port
 5500                          2     000f-e200-5300  5500-EI 28-Port
 4500                          3     000f-e200-5104  4500 50-Port
```

```
 4200G                       2     000f-e200-2420  4200G 12-Port
Processing...please wait
%Apr  3 08:12:37:813 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-2200 is joined in cluster aaa.

%Apr  3 08:12:37:831 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-0000 is joined in cluster aaa.

%Apr  3 08:12:37:847 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-7800 is joined in cluster aaa.

%Apr  3 08:12:37:863 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-2420 is joined in cluster aaa.

%Apr  3 08:12:37:996 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e202-2180 is joined in cluster aaa.

%Apr  3 08:12:38:113 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 0016-e0c0-c201 is joined in cluster aaa.

%Apr  3 08:12:38:139 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-5104 is joined in cluster aaa.

%Apr  3 08:12:38:367 2000 aaa_0.Sysname CLST/5/LOG:- 1 -
Member 000f-e200-5300 is joined in cluster aaa.

Cluster auto-build Finish!
 8 member(s) added successfully.
[aaa_0.Sysname-cluster]
```

build

Syntax

build *name*

undo build

View

Cluster view

Parameters

name: Name to be set for the cluster, a string of up to 8 characters, which can only be alphanumeric characters, minus signs (-), and underscores (_).

Description

Use the **build** command to build a cluster with a cluster name or change the cluster name.

Use the **undo build** command to remove the cluster.

You can use this command on a candidate device as well as on a management device.

Executing the **build** command on a candidate device will change the device to a management device and assign a name to the cluster created on the device, and the member number of the management device is 0.

Executing the **build** command on a management device will change the cluster name.

Different from the **auto-build** command, the **build** command only builds a cluster on the management device, which will not immediately collect the topology information to add the candidate devices into the cluster, but wait for an interval (configured through the **ntdp timer** command) before it starts the topology collection.

Note

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4200G series Ethernet switches provide the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On the management device, the preceding functions are implemented as follows:

- When you create a cluster by using the **build** or **auto-build** command, UDP port 40000 is opened at the same time.
- When you remove a cluster by using the **undo build** or **undo cluster enable** command, UDP port 40000 is closed at the same time.

On member devices, the preceding functions are implemented as follows:

- When you execute the **add-member** command on the management device to add a candidate device to a cluster, the candidate device changes to a member device and its UDP port 40000 is opened at the same time.
- When you execute the **auto-build** command on the management device to have the system automatically add candidate devices to a cluster, the candidate devices change to member devices and their UDP port 40000 is opened at the same time.
- When you execute the **administrator-address** command on a device, the device's UDP port 40000 is opened at the same time.
- When you execute the **delete-member** command on the management device to remove a member device from a cluster, the member device's UDP port 40000 is closed at the same time.
- When you execute the **undo build** command on the management device to remove a cluster, UDP port 40000 of all the member devices in the cluster is closed at the same time.
- When you execute the **undo administrator-address** command on a member device, UDP port 40000 of the member device is closed at the same time.

Examples

Configure the current switch as a management device and set the cluster name to **aaa**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] cluster
[Sysname-cluster] build aaa
There is no base topology, if set up from local flash file?(Y/N)
```

```
n
#Apr  2 07:27:21:280 2000 aaa_0.4200G CLST/5/Cluster_Trap:- 1 -
OID:1.3.6.1.4.1.43.45.1.6.7.1.0.3(hgmpMemberStatusChange):member
00.00.00.00.00.e0.fc.00.51.00  role  change,  NTDPIndex:0.00.00.00.00.00.e0.fc.00.51.00,
Role:1
[aaa_0.Sysname-cluster]
```

cluster

Syntax

cluster

View

System view

Parameters

None

Description

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

Examples

Enter cluster view.

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

cluster enable

Syntax

cluster enable

undo cluster enable

View

System view

Parameters

None

Description

Use the **cluster enable** command to enable the cluster function.

Use the **undo cluster enable** command to disable the cluster function.

By default, the cluster function is enabled.

Note that:

- To create a cluster on a management device through the **build** command or the **auto-build** command, you must first enable the cluster function by executing the **cluster enable** command.
- When you execute the **undo cluster enable** command on the management device, the cluster function is disabled on the device, and the device stops operating as a management device, and the cluster and all its members are removed.
- When you execute the **undo cluster enable** command on a member device, the cluster function is disabled on the device, and the device leaves the cluster.
- When you execute **undo cluster enable** command on a device that does not belong to any cluster, the cluster function is disabled on the device, and thus you cannot create a cluster on the device or add the device to an existing cluster.

Examples

Enable the cluster function on the switch.

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

cluster switch-to

Syntax

cluster switch-to { *member-number* | **mac-address** *H-H-H* | **administrator** | **sysname** *sysname* }

View

User view

Parameters

member-number: Member number of a member device, ranging from 1 to 255.

mac-address *H-H-H*: Specifies the MAC address of a member device.

administrator: Switches back from the member device to the management device.

sysname *sysname*: Specifies the system name of a member device, *sysname* is a string of 1 to 30 characters.

Description

Use the **cluster switch-to** command to switch between the management device and a member device for configuration and management.

On the management device, you can switch to the view of a member device to configure and manage the member device, and then switch back to the management device.

Both switching directions (from the management device to a member device, and from a member device to the management device) will use Telnet connection. Switching is performed based on the following rules:

- Both switching directions will perform authentication. In a switching process, the system will authenticate the level-3 super password. If the super password on the device that requests the switching is inconsistent with that on the requested device, the switching fails. When a candidate device joins the cluster, its super password will automatically synchronize to the supper password on the management device (this is not true when you add the candidate device to the cluster using the **administrator-address** command). It is recommended not to change the super password of

any cluster member or the management device, so as to avoid switching failure resulting from authentication failure.

- After you switch from the management device to a member device, the member device view will inherit the user privilege level of the current management device view.
- After you switch from a member device to the management device, the privilege level on the management device view will be determined by the configuration on the management device.
- If all the Telnet resources on the requested device are used up, the switching to the device will not succeed.

When you execute this command on the management device with an inexistent member number or a MAC address that is not in the member list, an error will occur. In this case, you can enter **quit** to end the switching.

Examples

Switch from the management device to number-6 member device and then switch back to the management device.

```
<aaa_0.Sysname> cluster switch-to 6
<aaa_6.Sysname> quit
<aaa_0.Sysname>
```

cluster-local-user

Syntax

cluster-local-user *username* **password** { **cipher** | **simple** } *password*

undo cluster-local-user *username*

View

Cluster view

Parameters

username: Name of the public local user for the cluster, a string of 1 to 55 characters.

cipher: Cipher text password.

simple: Plain text password.

password: Password of the public local user for the cluster. If the password is in cipher text, the value is a string of 1 to 63 characters; if the password is in plain text, the value is a string of 1 to 63 characters or a string of 88 characters.

Description

Use the **cluster-local-user** command to create a public local user for the cluster. The username and password are used to manage all member devices through Web.

Use the **undo cluster-local-user** command to remove all public local user configurations for the cluster.

By default, no public local user is configured for the cluster.

- You can use this command only on the management device to create only one public local user.
- When you configure this command on the management device, the configuration will be synchronized to the member devices that have passed the authentication; when a new member

device passes the authentication, this configuration is synchronized to the new member automatically. If a user with the same name already exists, the new configuration will overwrite the old one.

- If a member device leaves the cluster, the public local user configurations will not be removed.

Examples

On the management device, create a public local user for the cluster: the username is **public**; the password is **123** in plain text.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-local-user public password simple 123
```

cluster-mac

Syntax

cluster-mac *H-H-H*

undo cluster-mac

View

Cluster view

Parameters

H-H-H: Multicast MAC address to be set for the cluster, in hexadecimal format. This argument can be one of the following addresses: 0180-C200-0000, 0180-C200-000A, 0180-C200-0020 to 0180-C200-002F.

Description

Use the **cluster-mac** command to configure a multicast destination MAC address for HGMPv2 protocol packets.

Use the **undo cluster-mac** command to restore the default multicast destination MAC address of HGMPv2 protocol packets.

The default multicast destination MAC address of HGMPv2 protocol packets is 0180-C200-000A.

Note that you can only use this command on a management device.

With the destination MAC address of HGMPv2 protocol packets configured on the management device, through the multicast MAC synchronization packets, the member devices can learn the multicast MAC address of HGMPv2 protocol packets and use it to send NDP multicast packets, NTDP multicast packets, and cluster packets.

Since some devices cannot forward the multicast packets with the destination MAC address of 0180-C200-000A, HGMPv2 packets cannot traverse these devices. For a cluster to work normally in this case, you can modify the multicast destination MAC address of HGMPv2 protocol packets without changing the current networking.

Related commands: **cluster-mac syn-interval**.

Examples

Configure multicast MAC address 0180-C200-0028 for HGMPv2 protocol packets.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-mac 0180-C200-0028
```

cluster-mac syn-interval

Syntax

cluster-mac syn-interval *time-interval*

View

Cluster view

Parameters

time-interval: Interval to send multicast MAC synchronization packets, ranging from 0 to 30 minutes.

Description

Use the **cluster-mac syn-interval** command to set the interval for the management device to send HGMP V2 multicast MAC synchronization packets periodically. You can only use this command on a management device.

By default, this interval is one minute.

HGMPv2 multicast MAC synchronization packets are used for synchronizing the HGMPv2 multicast MAC address configuration (configured through the **cluster-mac** command) between devices in a cluster, so that HGMPv2 protocol packets can be forwarded normally within the cluster. HGMPv2 multicast MAC synchronization packets are Layer 2 multicast packets.

If you set this interval to zero on a management device, the management device will not send HGMP V2 multicast MAC synchronization packets to other devices.

Related commands: **cluster-mac**.

Examples

Set the interval for the management device to send HGMP V2 multicast MAC synchronization packets to one minute.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-mac syn-interval 1
```

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

Parameters

read: Indicates that the community has read-only access right to management information base (MIB) objects, that is, an SNMP network management station (NMS) can only query MIBs for device information when it uses this community name to access the agent.

write: Indicates that the community has read-write access right to MIB objects, that is, an SNMP NMS is capable of configuring the devices when it uses this community name to access the agent.

community-name: Community name, a string of 1 to 27 characters.

view-name: MIB view name, a string of 1 to 32 characters. The default view is ViewDefault.

Description

Use the **cluster-snmp-agent community** command to create a public SNMP community for the cluster.

Use the **undo cluster-snmp-agent community** command to remove the configuration.

By default, no public SNMP community is configured for a cluster.

- You can use this command only in cluster view on the management device to create only one public community for the cluster.
- When you configure this command on the management device, the configuration is synchronized to the member devices that have passed the authentication; when a new member device passes the authentication, this configuration is synchronized to the new member automatically. If a community with the same name already exists, the new configuration will overwrite the old one.
- If a member device leaves the cluster, the synchronized SNMP configurations will not be removed.

Note

For the SNMP configurations, refer to the *SNMP-RMON Operation* part in this manual.

Examples

On the management device, create a public SNMP community with the name of **access**, allowing read-only access right using this community name.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent community read access
```

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

Parameters

v3: SNMPv3.

group-name: Group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMP group as authentication only (without privacy).

privacy: Specifies the security model of the SNMP group as authentication and privacy.

read-view *read-view*: Read view, a string of 1 to 32 characters. The default read view is ViewDefault.

write-view *write-view:* Write view, a string of 1 to 32 characters. By default, no write view is configured, namely, the NMS cannot perform the write operations to all MIB objects on the device.

notify-view *notify-view*: Notify view, for sending traps, a string of 1 to 32 characters. By default, no notify view is configured, namely, the agent does not send traps to the NMS.

Description

Use the **cluster-snmp-agent group v3** command to create a public SNMP group for a cluster. This configuration is effective to all cluster members that have passed the authentication.

Use the **undo cluster-snmp-agent group v3** command to remove the public SNMP group for the cluster.

By default, no public SNMP group is configured for a cluster.

- You can use this command only in cluster view on the management device to create only one public group for the cluster.
- When you configure this command on the management device, the configuration is synchronized to the member devices that have passed the authentication; when a new member device passes the authentication, this configuration is synchronized to the new member automatically. If a group with the same name already exists, the new configuration will overwrite the old one.
- If a member device leaves the cluster, the synchronized SNMP configurations will not be removed.

Note

For the SNMP configurations, refer to the *SNMP-RMON Operation* part in this manual.

Examples

Create a public SNMP group with the name of **snmpgroup**.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent group v3 snmpgroup
```

cluster-snmp-agent mib-view included

Syntax

cluster-snmp-agent mib-view included *view-name oid-tree*

undo cluster-snmp-agent mib-view *view-name*

View

Cluster view

Parameters

view-name: View name, a string of 1 to 32 characters. The default view is ViewDefault.

oid-tree: MIB subtree, identified by the OID of the subtree root node or the name of the subtree root node. The value is a string of 1 to 255 characters.

included: Indicates that all nodes of the MIB tree are included in the current view.

Description

Use the **cluster-snmp-agent mib-view** command to create or update the public MIB view information for the cluster.

Use the **undo cluster-snmp-agent mib-view** command to remove the current configuration.

By default, public MIB view for the cluster is ViewDefault. When you access the device through the ViewDefault view, you can access all the MIB objects of the iso subtree with the OID of 1.

- You can use this command only in cluster view on the management device to create only one public MIB view for the cluster.
- When you configure this command on the management device, the configuration is synchronized to the member devices that have passed the authentication; when a new member device passes the authentication, this configuration is synchronized to the new member automatically. This configuration is effective to all cluster members that have passed the authentication.
- If a member device leaves the cluster, the synchronized SNMP configurations will not be removed.

Note

For the SNMP configurations, refer to the *SNMP-RMON Operation* part in this manual.

Examples

Create a public MIB view **mib2**, which includes all objects of the subtree **mib-2**.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[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 *username groupname* [**authentication-mode** { **md5** | **sha** } *authpassstring* [**privacy-mode** { **des56** *privpassstring* }]]

undo cluster-snmp-agent usm-user v3 *username groupname*

View

Cluster view

Parameters

v3: SNMPv3.

username: User name, a string of 1 to 32 characters.

groupname: Group name, a string of 1 to 32 characters.

authentication-mode: Specifies the security model as authentication. If you do not provide this keyword, the security model defaults to no authentication no privacy.

md5: Specifies the authentication protocol as MD5. MD5 generates a 128-bit message digest and it is faster than SHA.

sha: Specifies the authentication protocol as SHA. SHA generates a 160-bit message digest and it provides a higher security than MD5.

authpassstring: Authentication password. For a plain text password, the value is a string of 1 to 16 characters. For a cipher text password, the value is a string of 1 to 24 characters.

privacy-mode: Specifies the security model as privacy.

des56: Specifies the privacy protocol as data encryption standard (DES).

privpassstring: The privacy password. For a plain text password, the value is a string of 1 to 16 characters. For a cipher text password, the value is a string of 1 to 24 characters.

Description

Use the **cluster-snmp-agent usm-user v3** command to add a new user to the public SNMPv3 group of the cluster.

Use the **undo cluster-snmp-agent usm-user v3** command to delete the public SNMPv3 user of the cluster.

By default, no public SNMPv3 user is configured for the cluster.

- You can use this command only in cluster view on the management device to add only one public SNMPv3 group user for the cluster.
- When you configure this command on the management device, the configuration is synchronized to the member devices that have passed the authentication; when a new member device passes the authentication, this configuration is synchronized to the new member automatically. If a user with the same name already exists, the new configuration will overwrite the old one.
- If a member device leaves the cluster, the synchronized SNMP configurations will not be removed.

Examples

Add a user **wang** to the SNMPv3 group **huawei**. Configure the security model as **authentication without privacy**, the authentication protocol as **MD5**, the plain-text authentication password as **pass**.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent usm-user v3 wang huawei authentication-mode md5
pass
```

delete-member

Syntax

delete-member *member-id* [**to-black-list**]

View

Cluster view

Parameters

member-id: Member number of a member device, ranging from 1 to 255.

to-black-list: Adds the device removed from a cluster to the blacklist to prevent it from being added to the cluster.

Description

Use the **delete-member** command to remove a member device from the cluster.

Note that a cluster will collect the topology information at the topology collection interval. If you do not add a device to the cluster blacklist when removing it from the cluster, the device will be added to the cluster again when the cluster collects topology information. Therefore, to remove a device from a cluster permanently, you can use the following methods:

- Use the **delete-member** command with the **to-black-list** keyword specified to remove a device and add the device to the blacklist of the cluster.
- Before using the **delete-member** command to remove a device from the cluster, use the **undo ndp enable** and **undo ntdp enable** command to disable NDP and NTDP on the ports of the device which connect with the cluster member devices.

Note

This command is applicable to management devices only.

Related commands: **add-member**.

Examples

Remove the member device numbered 4 from the cluster, and add it to the cluster blacklist.

```
<aaa_0.Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] delete-member 4 to-black-list
```

display cluster

Syntax

display cluster

View

Any view

Parameters

None

Description

Use the **display cluster** command to display the status and statistics information of the cluster to which the current switch belongs.

Executing this command on a member device will display the following information: cluster name, member number of the current switch, MAC address and status of the management device, holdtime, and interval to send handshake packets.

Executing this command on a management device will display the following information: cluster name, number of the member devices in the cluster, cluster status, holdtime, and interval to send handshake packets.

Executing this command on a device that does not belong to any cluster will display an error.

Examples

Display cluster information on a management device.

```
<aaa_0.Sysname-cluster> display cluster
Cluster name:"aaa"
Role:Administrator
Management-vlan:100

Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:20.1.1.1/24
cluster-mac:0180-c200-000a
No logging host configured
No SNMP host configured
No FTP server configured
No TFTP server configured

1 administrator(s) in the cluster
 2 member(s) in the cluster, 0 of them down

 0 candidate(s) does not join the cluster
```

Display cluster information on a member device.

```
[aaa_2.4200G-3] display cluster
Cluster name:"aaa"
Role:Member
```

```
Member number:2
Management-vlan:100

cluster-mac:0180-c200-000a
Handshake timer:10 sec
Handshake hold-time:60 sec

Administrator device mac address:000f-e20f-3901
Administrator status:Up
```

Table 2-5 Description on the fields of the **display cluster** command

Field	Description
Cluster name	Name of the cluster, which can be configured through the **build** command
Role	Role of this switch
Management-vlan	Number of the management VLAN, which can be configured through the **management-vlan** command
Member number	Member number of this switch
Handshake timer	Interval to send handshake packets, which can be configured through the **timer** command
Handshake hold-time	Holdtime of the neighbor status information, which can be configured through the **holdtime** command
Administrator device mac address	MAC address of the management device
Administrator status	Status of the management device

display cluster candidates

Syntax

display cluster candidates [**mac-address** *H-H-H* | **verbose**]

View

Any view

Parameters

mac-address *H-H-H*: Specifies a candidate device by its MAC address. *H-H-H* represents the MAC address.

verbose: Displays detailed information about candidate devices.

Description

Use the **display cluster candidates** command to display information about one specified or all candidate devices of a cluster.

You can only use this command on a management device.

Note that, after a cluster is set up on an Switch 4200G series switch, the switch will collect the topology information of the network at the topology collection interval you set and automatically add the candidate devices it discovers into the cluster. As a result, if the topology collection interval is too short (the default interval is 1 minute), the switches acting as candidate devices will not keep in candidate state for a long time – they will change to member devices within a short time. If you do not want the candidate switches to be automatically added into the cluster, you can set the topology collection interval to zero (by using the **ntdp timer** command), which specifies not to perform topology collection periodically.

Examples

Display information about all candidate devices.

```
<aaa_0.Sysname-cluster> display cluster candidates
MAC             HOP  IP                  PLATFORM
3900-0000-3334  2    16.1.1.11/24        4200G
000f-e20f-3190  1    16.1.1.1/24         4200G
```

Table 2-6 Description on the fields of the **display cluster candidates** command

Field	Description
MAC	MAC address of the candidate device
Hop	Hops from the management device to the candidate device
IP	IP address of the candidate device
Platform	Platform of the candidate device

Display information about a specified candidate device.

```
<aaa_0.Sysname-cluster> display cluster candidates mac-address 000f-e20f-3190
Hostname  : 4200G
MAC       : 000f-e20f-3190
Hop       : 1
Platform  : 4200G 12-Port
IP        : 16.1.1.1/24
```

Display detailed information about all candidate devices.

```
<aaa_0.Sysname-cluster> display cluster candidates verbose

Hostname  : Sysname
MAC       : 5200-0000-3334
Hop       : 2
Platform  : 4200G 24-Port
IP        : 16.1.1.11/24


Hostname  : 4200G-1
MAC       : 000f-e20f-3190
Hop       : 1
Platform  : 4200G 48-Port
```

```
IP         : 16.1.1.1/24
```

Table 2-7 Description on the fields of display cluster candidates verbose

Field	Description
Hostname	Name of the candidate device
MAC	MAC address of the candidate device
Hop	Hops from the management device to the candidate device
IP	IP address of the candidate device
Platform	Platform of the candidate device

display cluster members

Syntax

display cluster members [*member-number* | **verbose**]

View

Any view

Parameters

member-number: Member number of a device, ranging from 0 to 255.

verbose: Displays detailed information about all the devices in a cluster.

Description

Use the **display cluster members** command to display information about one specific or all devices in a cluster.

This command is only applicable to a management device.

Examples

Display information about all devices in a cluster.

```
<aaa_0.Sysname-cluster> display cluster members
SN   Device              MAC Address     Status Name
0    4200G               000f-e20f-3901  Admin  aaa_0.Sysname
1    4200G               3900-0000-3334  Up     aaa_1.Sysname
2    4200G               000f-e20f-3190  Up     aaa_2.4200G-3
```

Table 2-8 Description on the fields of the **display cluster members** command

Field	Description
SN	Member number of a device in the cluster
Device	Device type
MAC Address	Device MAC address
Status	Device status
Name	Device name

Display detailed information about all devices in a cluster.

```
<aaa_0.Sysname-cluster> display cluster members verbose
Member number:0
Name:aaa_0.Sysname
Device: 4200G 12-Port
MAC Address:000f-e20f-3901
Member status:Admin

Hops to administrator device:0
IP: 100.100.1.1/24
Version:

   3Com Versatile Routing Platform Software
   Comware Software, Version 3Com OS V3.02.01s168
   Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
   Switch 4200G 12-Port 4200G

Member number:1
Name:aaa_1.3Com
Device: 4200G 24-Port
MAC Address:000f-e200-3334
Member status:Up
Hops to administrator device:2
IP: 16.1.1.11/24
Version:

   3Com Versatile Routing Platform Software
   Comware Software, Version 3Com OS V3.02.01s168
   Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
   Switch 4200G 24-Port 4200G

Member number:2
Name: aaa_2.3Com
Device: 4200G 12-Port
MAC Address:000f-e20f-3190
Member status:Up
Hops to administrator device:1
IP: 16.1.1.1/24
Version:
   3Com Versatile Routing Platform Software
   Comware Software, Version 3Com OS V3.02.01s168
   Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
   Switch 4200G 12-Port 4200G
```

Table 2-9 Description on the fields of display cluster members verbose

Field	Description
Member number	Member number of the device in the cluster
Name	Device name
Device	Device type
MAC Address	Device MAC address
Member status	Device status
Hops to administrator device	Hops from the device to the management device
IP	Device IP address
Version	Software version of the device

ftp cluster

Syntax

ftp cluster

View

User view

Parameters

None

Description

Use the **ftp cluster** command to connect to the shared FTP server of the cluster and enter FTP Client view through the management device.

You can use the **ftp-server** command on the management device to configure the shared FTP server of the cluster, which is used for software version update and configuration file backup of the cluster members.

Related commands: **ftp-server**.

Note

For how to access other FTP servers using the **ftp** command, refer to the *FTP-SFTP-TFTP* part of the manual.

Examples

Connect to the FTP server shared by the cluster.

```
<123_1.Sysname> ftp cluster
Trying ...
Press CTRL+K to abort
```

```
Connected.
220 FTP service ready.
User(none):hello
331 Password required for hello.
Password:
230 User logged in.
```

ftp-server

Syntax

ftp-server *ip-address*

undo ftp-server

View

Cluster view

Parameters

ip-address: IP address of the FTP server to be configured for the cluster.

Description

Use the **ftp-server** command to configure a shared FTP server for the cluster on the management device.

Use the **undo ftp-server** command to remove the shared FTP server setting.

By default, the management device acts as the shared FTP server of the cluster.

After you configure the IP address of the shared FTP server on the management device, the member devices in the cluster can access the shared FTP sever through the management device to back up configuration and download software. The IP address of the shared FTP server configured on the management device takes effect on the management device only and will not be applied to the member devices through the cluster management packets.

After the IP address of the shared FTP server is configured, network address translation (NAT) is enabled on the management device immediately. When a member device uses the **ftp cluster** command to access the shared FTP server, the management device will translate the private IP address of the member device to a public network address, forward the requests of the member device to the FTP server, and forward the responses of FTP server to the member device according to the NAT record.

Examples

Configure FTP server 1.0.0.9 on the management device of a cluster.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] ftp-server 1.0.0.9
```

holdtime

Syntax

holdtime *seconds*

undo holdtime

View

Cluster view

Parameters

seconds: Neighbor information holdtime in seconds, ranging from 1 to 255.

Description

Use the **holdtime** command to configure the neighbor information holdtime of the member switches.

Use the **undo holdtime** command to restore the default holdtime value.

By default, the neighbor information holdtime is 60 seconds.

Note that:

- If the management switch does not receive NDP information from a member device within the holdtime, it sets the state of the member device to “down”. When the management device receives the NDP information from the device again, the device will be re-added to the cluster automatically.
- If the management device receives NDP information form a member device within the holdtime, the member device stays in the normal state and does not need to be added to the cluster again.
- Note that, you need only execute the command on a management device, which will advertise the holdtime value to all member devices in the cluster.

Examples

Set the neighbor information holdtime of the cluster members to 30 seconds.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] holdtime 30
```

ip-pool

Syntax

ip-pool *administrator-ip-address* { *ip-mask* | *ip-mask-length* }

undo ip-pool

View

Cluster view

Parameters

administrator-ip-address: IP address for the device to be set as the management device of a cluster.

ip-mask: Mask of the cluster IP address pool.

ip-mask-length: Mask length of the cluster IP address pool.

Description

Use the **ip-pool** command to configure a private IP address pool on the management device.

Use the **undo ip-pool** command to cancel the IP address pool configuration.

Before creating a cluster, you must first configure a private IP address pool. When a candidate device joins a cluster, the management device dynamically assigns a private IP address in the pool to it, so that the candidate device can communicate with other devices in the cluster. This enables the management device to manage and maintain member devices in the cluster.

As the IP address pool of a cluster cannot be modified, be sure to execute these two commands before a cluster is created.

Examples

Configure a private IP address pool for a cluster.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] cluster
[Sysname-cluster] ip-pool 10.200.0.1 20
```

logging-host

Syntax

logging-host *ip-address*

undo logging-host

View

Cluster view

Parameters

ip-address: IP address of the device to be configured as the log host of a cluster.

Description

Use the **logging-host** command to configure a shared log host for a cluster on the management device.

Use the **undo logging-host** command to remove the shared log host setting.

By default, no shared log host is configured.

After setting the IP address of a log host for the cluster, the member devices in the cluster can send logs to the log host through the management device.

Note that you must execute the command on a management device.

For how to configure a switch to send logs to the log host, refer to *Information Center Operation*.

Examples

Configure the device with IP address 10.10.10.9 as the log host of a cluster.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
```

```
[aaa_0.Sysname-cluster] logging-host 10.10.10.9
```

management-vlan

Syntax

management-vlan *vlan-id*

undo management-vlan

View

System view

Parameters

vlan-id: ID of the VLAN to be specified as the management VLAN.

Description

Use the **management-vlan** command to specify the management VLAN on the switch.

Use the **undo management-vlan** command to restore the default management VLAN.

By default, VLAN 1 is used as the management VLAN.

When specifying the management VLAN, note that:

- The management VLANs on all the devices in a cluster must be the same.
- You can specify the management VLAN on a device only when no cluster is created on the device. You cannot change the management VLAN on a device that already joins a cluster. If you want to change the management VLAN on a device where a cluster has already been created, you must first remove the cluster configuration on the device, then re-specify a VLAN as the management VLAN, and finally re-created the cluster.
- The management VLAN of a cluster defaults to VLAN 1. To isolate cluster management packets from other packets to improve the cluster information security, it is recommended to configure the management VLAN of the cluster as another VLAN.

Examples

Specify VLAN 2 as the management VLAN of the current switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] management-vlan 2
```

management-vlan synchronization enable

Syntax

management-vlan synchronization enable

undo management-vlan synchronization enable

View

Cluster view

Parameters

None

Description

Use the **management-vlan synchronization enable** command to enable the management VLAN synchronization function for the cluster.

Use the **undo management-vlan synchronization enable** command to disable the function.

By default, the management VLAN synchronization function is enabled.

You can use this command only on the management device.

By enabling the management VLAN synchronization function on the management device, you can enable the management device to send a management VLAN synchronization packet to the connected devices periodically. After receiving the management VLAN synchronization packet, the managed devices set their own management VLANs according to the packet. In this way, all devices set the same management VLAN automatically. After the synchronization, the management device can add other devices to the cluster.

Examples

Enable management VLAN synchronization on the management device.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster]management-vlan synchronization enable
```

nm-interface Vlan-interface

Syntax

nm-interface Vlan-interface *vlan-interface-id*

View

Cluster view

Parameters

vlan-interface-id: VLAN interface ID, in the range 1 to 4094. The VLAN interface specified by this argument must have been configured with an IP address.

Description

Use the **nm-interface Vlan-interface** command to configure a network management (NM) interface on a management device.

After an NM interface is specified on the management device of a cluster, the network administrator can log onto the management device through the NM interface to manage the devices in the cluster.

Note

- By default, the management VLAN interface is used as the NM interface.
- There is only one NM interface on a management device; any newly configured NM interface will overwrite the old one.

Examples

Configure VLAN-interface 2 as the NM interface.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] cluster
[Sysname-cluster] nm-interface Vlan-interface 2
```

reboot member

Syntax

reboot member { *member-number* | **mac-address** *H-H-H* } [**eraseflash**]

View

Cluster view

Parameters

member-number: Member number of a member device, ranging from 1 to 255.

mac-address *H-H-H*: Specifies the MAC address of the member device to be rebooted.

eraseflash: Deletes the configuration file of the member device when the member device reboots.

Description

Use the **reboot member** command to reboot a specified member device on the management device.

When a member device is in trouble due to some configuration errors, you can use the remote control function on the management device to maintain the member device remotely. For example, from the management device, you can delete the configuration file on a member device and reboot the member device, and recover the device to the normal state with the backup configuration.

The **eraseflash** keyword specifies to delete the startup configuration file when the member device reboots.

Examples

Reboot number-2 member device.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] reboot member 2
```

snmp-host

Syntax

snmp-host *ip-address*

undo snmp-host

View

Cluster view

Parameters

ip-address: IP address of a SNMP network management station (NMS) to be configured for the cluster.

Description

Use the **snmp-host** command to configure a shared SNMP NMS for the cluster on the management device.

Use the **undo snmp-host** command to remove the shared SNMP NMS setting.

By default, no shared SNMP NMS is configured.

After setting the IP address of an SNMP NMS for the cluster, the member devices in the cluster can send trap messages to the SNMP NMS through the management device.

Note that, you can only use the commands on a management device.

For how to configure a switch to send trap messages to the SNMP NMS, refer to *Information Center Operation*.

Examples

Configure SNMP NMS address 1.0.0.9 on the management device for the cluster.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] snmp-host 1.0.0.9
```

tftp get

Syntax

tftp { **cluster |** *tftp-server* } **get** *source-file* [*destination-file*]

View

User view

Parameters

cluster: Downloads files through the shared TFTP server of the cluster.

tftp-server: IP address or host name of the TFTP server.

source-file: Name of the file to be downloaded from the shared TFTP server of the cluster.

destination-file: Name of the file to which the downloaded file will be saved on the switch.

Description

Use the **tftp get** command to download a file from a specific directory on the shared TFTP server to the switch.

You can use the **tftp-server** command on the management device to configure the shared TFTP server of the cluster, which is used for software version update and configuration file backup of the cluster members. For TFTP server rights and directory configuration, refer to the user guide of the TFTP server software.

Related commands: **tftp put**, **tftp-server**.

 **Note**

- You need to specify the **cluster** keyword completely in the command.
- For description of other parameters of the **tftp** command, refer to the *FTP-SFTP-TFTP* part of the manual.

Examples

Download file **LANSwitch.app** from the shared TFTP server of the cluster to the switch and save it as **vs.app**.

```
<123_1.Sysname> tftp cluster get LANSwitch.app vs.app
```

tftp put

Syntax

tftp { **cluster |** *tftp-server* } **put** *source-file* [*destination-file*]

View

User view

Parameters

cluster: Uploads files through the shared TFTP server of the cluster.

tftp-server: IP address or host name of the TFTP server.

source-file: File name to be uploaded to the shared TFTP server.

destination-file: Name of the file to which the uploaded file will be saved in the storage directory of the TFTP server.

Description

Use the **tftp put** command to upload a file from the switch to a specified directory on the TFTP server.

You can use the **tftp-server** command on the management device to configure the shared TFTP server of the cluster, which is used for software version update and configuration file backup of the cluster members. For TFTP server rights and directory configuration, refer to the user guide of the TFTP server software.

Related commands: **tftp get**,**tftp-server**.

Note

You need to specify the **cluster** keyword completely in the command.

Examples

Upload file **config.cfg** on the switch to the shared TFTP server of the cluster and save it as **temp.cfg**.

```
<123_1.Sysname> tftp cluster put config.cfg temp.cfg
```

tftp-server

Syntax

tftp-server *ip-address*

undo tftp-server

View

Cluster view

Parameters

ip-address: IP address of a TFTP server to be configured for the cluster.

Description

Use the **tftp-server** command to configure a shared TFTP server for the cluster on the management device.

Use the **undo tftp-server** command to remove the shared TFTP server setting.

By default, no shared TFTP server is configured.

After the IP address of the shared TFTP server is configured, NAT is enabled on the management device immediately. When a member device uses the **tftp cluster get** or **tftp cluster put** command to download or upload a file from the shared TFTP server, the management device translates the private IP address of the member device to a public network address, forwards the requests of the member device to the TFTP server, and forwards the responses of TFTP server to the member device according to the NAT record.

Note that you can only use the commands on a management device.

Examples

Configure shared TFTP server 1.0.0.9 on the management device for the cluster.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] tftp-server 1.0.0.9
```

timer

Syntax

timer *interval*

undo timer

View

Cluster view

Parameters

interval: Interval (in seconds) to send handshake packets. This argument ranges from 1 to 255.

Description

Use the **timer** command to set the interval between sending handshake packets.

Use the **undo timer** command to restore the default value of the interval.

By default, the interval between sending handshake packets is 10 seconds.

In a cluster, the management device keeps connections with the member devices through handshake packets. Through the periodic handshaking between the management and member devices, the management device monitors the member status and link status.

Note that, you need only execute the command on a management device, which will advertise the handshake interval setting to all member devices in the cluster.

Examples

Set the interval to send handshake packets to 3 seconds.

```
<aaa_0.Sysname> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] timer 3
```

tracemac

Syntax

tracemac { **by-mac** *mac-address* **vlan** *vlan-id* | **by-ip** *ip-address* } [**nondp**]

View

Any view

Parameters

by-mac: Specifies to trace a device through the specified destination MAC address.

mac-address: MAC address of the device to be traced.

vlan *vlan-id*: Specifies to trace a device in the specified VLAN. *vlan-id* ranges from 1 to 4094.

by-ip: Specifies to trace a device through the specified destination IP address.

ip-address: IP address of the device to be traced.

nondp: Specifies not to check the NDP neighbor information.

Description

Use the **tracemac** command to trace a device in a cluster through the specified destination MAC address or IP address, and to display the path from the current device to the destination device.

Note

- When using the destination IP address to trace a device, the switch looks up the ARP entry corresponding to the IP address, and then looks up the MAC address entry according to the ARP entry.
- If the queried IP address has a corresponding ARP entry, but the corresponding MAC address of the IP address does not exist in the MAC address table, the trace of the device fails.
- To trace a specific device using the **tracemac** command, make sure that all the devices passed support the **tracemac** function.
- To trace a specific device in a management VLAN using the **tracemac** command, make sure that all the devices passed are within the same management VLAN as the device to be traced.

Examples

Trace the device that belongs to VLAN 1 through its MAC address 00e0-f032-0005.

```
<aaa_0.Sysname> tracemac by-mac 000f-e232-0005 vlan 1
Tracing MAC address 000f-e232-0005 in vlan 1
1 000f-e232-0001  3Com01   GigabitEthernet1/0/2
2 000f-e232-0002  3Com02   GigabitEthernet1/0/7
3 000f-e232-0003  3Com03   GigabitEthernet1/0/4
4 000f-e232-0005  3Com05   Local
```

Trace the device that belongs to VLAN 1 through its IP address 192.168.1.5.

```
<aaa_0.Sysname> tracemac by-ip 192.168.1.5
Tracing MAC address 000f-e232-0005 in vlan 1
1 000f-e232-0001  3Com01   GigabitEthernet1/0/2
2 000f-e232-0002  3Com02   GigabitEthernet1/0/7
3 000f-e232-0003  3Com03   GigabitEthernet1/0/4
4 000f-e232-0005  3Com05   Local
```

Enhanced Cluster Feature Configuration Commands

black-list

Syntax

black-list add-mac *mac-address*

black-list delete-mac { **all** | *mac-address* }

View

Cluster view

Parameters

mac-address: MAC address of the device to be added to the blacklist. The format is *H-H-H*, for example, 0100-0498-e001.

all: Deletes all MAC address in the current cluster blacklist.

Description

Use the **black-list add-mac** command to add the specified MAC address to the cluster blacklist, so that the device with the specified MAC address cannot join the cluster.

Use the **black-list delete-mac** command to remove all the MAC addresses or the specified MAC address from the current cluster blacklist, so that all devices or the device with the specified MAC address can join the cluster.

By default, no MAC address is added to the cluster blacklist.

Note

You can only use this command on the cluster administrative device.

If the device to be added to the blacklist is a member of the cluster, the execution of the **black-list add-mac** command will remove the device from the cluster and then add it to the cluster blacklist. In this case, the **black-list add-mac** command is equivalent to the **delete-member** *member-id* **to-black-list** command.

Examples

Add the device with the MAC address 0010-3500-e001 to the blacklist.

```
<aaa_0.Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] black-list add-mac 0010-3500-e001
```

Delete all addresses in the current cluster blacklist.

```
[aaa_0.Sysname-cluster] black-list delete-mac all
```

display cluster base-members

Syntax

display cluster base-members

View

Any view

Parameters

None

Description

Use the **display cluster base-members** command to display the information about all the devices in the base cluster topology, such as member number, name, MAC address, and the current status of each device in a cluster.

Examples

Display the information about all the devices in the base cluster topology.

```
<aaa_0.Sysname> display cluster base-members
SN          Device                          MAC Adress      Status
0           aaa_0.Sysname                   000f-e200-30a0  UP
1           aaa_1.4200G                     000f-e200-86e4  UP
```

Table 2-10 Description on the fields of **display cluster base-members**

Field	Description
SN	Device number in the cluster
Device	Device name
MAC Address	Device MAC address
Status	Device status Up: The member is connected. Down: The member is disconnected.

display cluster base-topology

Syntax

display cluster base-topology [**mac-address** *mac-address* | **member** *member-id*]

View

Any view

Parameters

mac-address *mac-address*: Displays the structure of the standard topology three layers above or below the node specified by the MAC address.

member *member-id*: Displays the structure of the standard topology three layers above or below the node specified by the member ID.

Description

Use the **display cluster base-topology** command to display the standard topology of the cluster.

The standard topology of a cluster refers to the topology saved through the **topology save-to** command. The standard topology is the backup of the normal topology information of a cluster and is mainly used to resume the normal topology of the cluster member devices in case the cluster topology encounters a fault.

Examples

Display the standard topology of the cluster.

```
<aaa_0.Sysname> display cluster base-topology
-------------------------------------------------------------------------
     (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-------------------------------------------------------------------------
[aaa_0.Sysname:000f-e202-2180]
     |
     ├-(P_0/40)<-->(P_0/6)[Sysname:000f-e200-2200]
     |
     ├-(P_0/28)<-->(P_3/0/1)[Sysname:000f-e200-1774]
     |
     ├-(P_0/22)<-->(P_1/0/2)[aaa_5.Sysname:000f-e200-5111]
     |
     ├-(P_0/18)<-->(P_3/0/2)[Sysname 4200G:000f-e218-d0d0]
     |
     ├-(P_0/14)<-->(P_1/0/2)[Sysname:000f-e200-5601]
     |
     └-(P_0/4)<-->(P_0/2)[4200G:000f-e200-00cc]
```

The output information of the **display cluster base-topology** command is in the following format:

(peer port number)<-->(local port number)[peer device name:peer device MAC address]

For example, (P_0/40)<-->(P_0/6)[Sysname:000f-e200-2200] means that the peer device uses its port GigabitEthernet 1/0/40 to connect to port GigabitEthernet 1/0/6 of the local device; the peer device name is Sysname; the MAC address of the peer device is 000f-e200-2200.

display cluster black-list

Syntax

display cluster black-list

View

Any view

Parameters

None

Description

Use the **display cluster black-list** command to display the information of devices in the current cluster blacklist.

Related commands: **black-list**.

Examples

Display the contents of the current cluster blacklist.

```
<aaa_0.Sysname> display cluster black-list
  Device ID           Access Device ID           Access port
  000f-e200-5502      000f-e202-2180             GigabitEthernet1/0/24
  00e0-fd34-bc66      000f-e202-2180             GigabitEthernet1/0/1
```

Table 2-11 Description on the fields of the **display cluster black-list** command

Field	Description
Device ID	ID of the device in the blacklist, expressed by the MAC address of the device
Access Device ID	ID of the device (in the cluster) that is connected with a device in the blacklist, expressed by the MAC address of the device
Access port	Port (in the cluster) that is connected with a device in the blacklist

display cluster current-topology

Syntax

display cluster current-topology [**mac-address** *mac-address1* [**to-mac-address** *mac-address2*] | **member-id** *member-id1* [**to-member-id** *member-id2*]]

View

Any view

Parameters

mac-address *mac-address1*: Displays the topology structure three layers above or below the node specified by the MAC address. If **to-mac-address** is specified, *mac-address1* is the start point of the route in the specified route topology displayed.

to-mac-address *mac-address2*: Displays the topology structure of the route from *mac-address1 to mac-address2*.

member-id *member-id1*: Displays the structure of the standard topology three layers above or below the node specified by the member ID. If **to-member-id** is specified, *member-id1* is the start point of the route in the specified route topology displayed.

to-member-id *member-id2*: Displays the topology structure of the route from *member-id1 to member-id2*.

Description

Use the **display cluster current-topology** command to display the topology of the current cluster.

If **to-mac-address** or **to-member-id** is not specified, the system displays the topology structure three layers below the node specified by the MAC address or member ID.

If **to-mac-address** or **to-member-id** is specified, the system displays the topology structure of the route between the two specified MAC addresses or two member IDs.

Note

When you display the cluster topology information, the devices attached to the switch that is listed in the backlist will not be displayed.

Examples

Display the topology of the current cluster.

```
<aaa_0.Sysname> display cluster current-topology
-------------------------------------------------------------------------
     (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-------------------------------------------------------------------------
ConnectFlag:
     <--> normal connect      ---> odd connect     **** in blacklist
     ???? lost device         ++++ new device      -┤├- STP discarding
-------------------------------------------------------------------------
[aaa_0.Sysname:000f-e202-2180]
    |
    ├-(P_0/40)<-->(P_0/6)[Sysname:000f-e200-2200]
    |
    ├-(P_0/28)<-->(P_3/0/1)[Sysname:000f-e200-1774]
    |
    ├-(P_0/24)****(P_1/0/6)[clie:000f-e200-5502]
    |
    ├-(P_0/22)<-->(P_1/0/2)[aaa_5.Sysname:000f-e200-5111]
    |
    ├-(P_0/18)<-->(P_3/0/2)[Sysname 4500:000f-e218-d0d0]
    |
    ├-(P_0/14)<-->(P_1/0/2)[Sysname:000f-e200-5601]
    |
    ├-(P_0/10)<-->(P_1/0/1)[aaa_7.4200G:0012-a990-2241]
    |
    ├-(P_0/4)<-->(P_0/2)[5500-EI:000f-e200-00cc]
    |
    └-(P_0/1)****(P_0/1)[Sysname:00e0-fd34-bc66]
```

display ntdp single-device mac-address

Syntax

display ntdp single-device mac-address *mac-address*

View

Any view

Parameters

mac-address: MAC address of the device whose detailed information is to be displayed.

Description

Use the **display ntdp single-device mac-address** command to display the detailed information, which is collected through NTDP protocol packets, about a single device. The information displayed by the command is similar to that displayed by the **display cluster members** command. However, if you want to display information about a device that is enabled with only NTDP and is not in any cluster, you have to use the **display ntdp single-device mac-address** command.

Examples

Display the detailed information about the switch with the MAC address 000f-e200-3956.

```
<Sysname> display ntdp single-device mac-address 000f-e200-3956

 Hostname  : aaa_0.4200G
 MAC       : 00e0-fc00-5200
 Hop       : 0
 Platform  : 4200G 12-Port
 IP        : 192.168.0.91/16
 Version   :
   3Com Versatile Routing Platform Software
   Comware Software, Version 3Com OS V3.02.01s168
   Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
   Switch 4200G 12-Port 4200G

 Cluster   :  Administrator switch of cluster aaa
 Stack     :  Candidate switch

 Peer MAC        Peer Port ID            Native Port ID          Speed Duplex
 00e0-fc02-2180  GigabitEthernet1/0/9    GigabitEthernet1/0/5    100   FULL
 00e0-fc00-5104  GigabitEthernet1/0/16   GigabitEthernet1/0/2    1000  FULL
```

Table 2-12 Description on the fields of the **display ntdp single-device** command

Field	Description
Hostname	System name of a device
MAC	MAC address of the device
Hop	Number of hops from the device to the topology-collecting device
Platform	Platform information of the device
IP	IP address and mask length of the management VLAN interface of the device
Version	Version information
Cluster	Role the device plays in the cluster
Peer MAC	MAC address of the peer device
Peer Port ID	Name of the port on the peer device connecting to the local device
Native Port ID	Name of the port on the local device connecting to the peer device
Speed	Rate of the local port connecting to the peer device
Duplex	Duplex mode of the local port connecting to the peer device

topology accept

Syntax

topology accept { **all** [**save-to local-flash**] | **mac-address** *mac-address* | **member-id** *member-id* | **administrator** }

View

Cluster view

Parameters

all: Accepts the current cluster topology as the standard topology.

save-to: Saves the standard topology of the current cluster to the local Flash or the cluster FTP server.

local-flash: Saves the standard topology of the current cluster to the local Flash.

mac-address *mac-address*: Accepts adding the device with the specified MAC address to the standard topology of the cluster.

member-id *member-id*: Accepts adding the device with the specified member ID to the standard topology of the cluster.

administrator: Accepts adding the administrative device to the standard topology of the cluster.

Description

Use the **topology accept** command to accept the topology of the current cluster as the standard topology, and save the standard topology to the Flash memory of the administrative device so that the standard topology can be restored when errors occur to the topology.

Note

You can only use this command on the cluster management device.

Related commands: **display cluster base-topology**, **topology restore-from**, **topology save-to**.

Examples

Save the current cluster topology as the base topology and save it in the local flash.

```
<aaa_0.Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] topology accept all save-to local-flash
```

Accept the device with the MAC address 0010-0f66-3022 as a member of the base cluster topology.

```
<aaa_0.Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] topology accept mac-address 0010-0f66-3022
```

topology restore-from

Syntax

topology restore-from local-flash

View

Cluster view

Parameters

local-flash: Restores the standard topology of the cluster from the local Flash memory.

Description

Use the **topology restore-from** command to restore the standard topology of the cluster from the Flash memory of the administrative device when errors occur to the topology, and advertise the topology to the member devices of the cluster to ensure normal operation of the cluster.

Note

You can only use this command on the cluster administrative device.

Related commands: **topology accept**, **topology save-to**.

Examples

Restore the base cluster topology from the flash of the management device in the cluster.

```
<aaa_0.Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] topology restore-from local-flash
```

topology save-to

Syntax

topology save-to local-flash

View

Cluster view

Parameters

None

Description

Use the **topology save-to** command to save the standard topology of the cluster to the local Flash memory.

The file name used to save the standard topology is **topology.top**. Do not modify the file name.

Note

This command is applicable to only the management device of a cluster.

Related commands: **topology restore-from**.

Examples

Enter Cluster view.

```
<aaa_0.Sysname>system-view
System View: return to User View with Ctrl+Z.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster]
```

Save the standard topology of the cluster to the local Flash.

```
[aaa_0.Sysname-cluster] topology save-to local-flash
Base topology backup to file OK
```

Table of Contents

1 SNMP Configuration Commands

SNMP Configuration Commands

display snmp-agent

Syntax

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

View

Any view

Parameters

local-engineid: Displays the local SNMP entity engine ID.

remote-engineid: Displays all the remote SNMP entity engine IDs. At present, the device does not support application of the keyword.

Description

Use the **display snmp-agent** command to display the local SNMP entity engine ID or all the remote SNMP entity engine IDs.

Each device managed by the NMS needs a unique engine ID to identify an SNMP agent. By default, each device has a default engine ID. You should ensure that each engine ID is unique within an SNMP domain.

The creation of username and generation of cipher text password are related to engine ID in SNMPv3. If you change an engine ID, the username and password configured on the agent with this engine ID become invalid.

You can use the **snmp-agent local-engineid** command to configure an engine ID for the device.

Examples

Display the local SNMP entity engine ID.

```
<Sysname> display snmp-agent local-engineid
   SNMP local EngineID: 800007DB000FE20F12346877
```

SNMP local EngineID in the above information represents the local SNMP entity engine ID.

display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

View

Any view

Parameters

read: Displays the information about the SNMP communities with read-only permission.

write: Displays the information about the SNMP communities with read-write permission.

Description

Use the **display snmp-agent community** command to display the information about the SNMPv1/SNMPv2c communities with the specific access permission.

SNMPv1 and SNMPv2c use community name authentication. Therefore, the SNMPv1 and SNMPv2c messages carry community names; if the carried community names are not permitted by the NMS/agent, the messages will be discarded.

You need to create a read community name and a write community name separately, and these two kinds of community names on the NMS and on the device should be consistent.

If you execute the command when the SNMP agent is not started, the device prompts “SNMP Agent disabled”.

To display the current configuration username information of SNMPv3, use the **display snmp-agent usm-user** command.

Examples

Display the information about all the existing SNMPv1/SNMPv2c communities.

```
<Sysname> display snmp-agent community
   Community name:public
       Group name:public
       Storage-type: nonVolatile

   Community name:private
       Group name:private
       Storage-type: nonVolatile
```

Table 1-1 display snmp-agent community command output description

Field	Description
Community name	Community name SNMPv1 and SNMPv2c use community name authentication. A community name functions like a password; it is used to restrict access between the NMS and the agent.
Group name	Group name If you use the **snmp-agent community** command to configure a community name for SNMPv1 or SNMPv2c, the group name is the community name. If you use the **snmp-agent usm-user** { **v1** | **v2c** } command to configure a username, the group name is the group to which the user belongs, and the corresponding community name has the attribute of the group.

Field	Description
Storage-type	Storage type, which can be: • volatile: Information will be lost if the system is rebooted • nonVolatile: Information will not be lost if the system is rebooted • permanent: Modification is permitted, but deletion is forbidden • readOnly: Read only, that is, no modification, no deletion • other: Other storage types

display snmp-agent group

Syntax

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

View

Any view

Parameters

group-name: Name of the desired SNMP group, a string of 1 to 32 characters.

Description

Use the **display snmp-agent group** command to display the information about an SNMP group, including group name, security mode, related views, and storage mode.

A group is used to define security mode and related views. Users in the same group have the common attributes.

Security mode falls into three types: authPriv (authentication with privacy), authNoPriv (authentication without privacy), noAuthNoPriv (no authentication no privacy).

Related views include: read MIB view, write MIB view, and MIB view in which traps can be sent.

For the configuration of an SNMP group, refer to the **snmp-agent group** command.

Examples

Display the information about all the SNMP groups.

```
<Sysname> display snmp-agent group
   Group name: v3group
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: ViewDefault
       Notifyview : ViewDefault
       Storage-type: nonVolatile
```

Table 1-2 display snmp-agent group command output description

Field	Description
Group name	SNMP group name of the user
Security model	SNMP group security mode, which can be AuthPriv (authentication with privacy), AuthnoPriv (authentication without privacy), and noAuthnoPriv (no authentication no privacy).
Readview	Read-only MIB view corresponding to the SNMP group
Writeview	Writable MIB view corresponding to the SNMP group
Notifyview	Notify MIB view in which traps can be sent. It corresponds to the SNMP group
storage-type	Storage type, which can be: • volatile: Information will be lost if the system is rebooted • nonVolatile: Information will not be lost if the system is rebooted • permanent: Modification is permitted, but deletion is forbidden • readOnly: Read only, that is, no modification, no deletion • other: Other storage types

display snmp-agent mib-view

Syntax

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

View

Any view

Parameters

exclude: Specifies the SNMP MIB views that are of the excluded type.

Include: Specifies the SNMP MIB views that are of the included type.

view-name: Name of an SNMP MIB view to be displayed.

Description

Use the **display snmp-agent mib-view** command to display the MIB view configuration of the current Ethernet switch, including view name, MIB subtree, subtree mask, and so on.

For the description of the configuration items of MIB view, refer to the related description in the **snmp-agent mib-view** command.

Examples

Display the information about the currently configured MIB view.

```
<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
```

The above output information indicates that MIB view **ViewDefault** includes all MIB objects under the ISO MIB subtree except snmpUsmMIB, snmpVacmMIB and snmpModules.18.

display snmp-agent statistics

Syntax

display snmp-agent statistics

View

Any view

Parameters

None

Description

Use the **display snmp-agent statistics** command to display the statistics on SNMP packets.

The statistics are collected from the time when the switch is started, and the statistics will not be cleared if the SNMP is restarted.

If you execute the command when SNMP agent is not started, the device prompts “SNMP Agent disabled”.

Examples

Display the statistics on SNMP packets.

```
<Sysname> display snmp-agent statistics
  1276 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used a SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  1291 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  7 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
  3669 MIB objects retrieved successfully
  26 MIB objects altered successfully
  420 GetRequest-PDU accepted and processed
  832 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
  1276 GetResponse-PDU accepted and processed
  24 SetRequest-PDU accepted and processed
  15 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs droped silently
  0 Forwarded Confirmed Class PDUs droped silently
```

Table 1-3 display snmp-agent statistics command output description

Field	Description
Messages delivered to the SNMP entity	The total number of messages delivered to the SNMP entity from the transport service.
Messages which were for an unsupported version	The total number of SNMP messages delivered to the SNMP protocol entity and were for an unsupported SNMP version.
Messages which used a SNMP community name not known	The total number of SNMP messages delivered to the SNMP protocol entity which used an SNMP community name not known to said entity.
Messages which represented an illegal operation for the community supplied	The total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASN.1 or BER errors in the process of decoding	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.
Messages passed from the SNMP entity	The total number of SNMP messages which were passed from the SNMP protocol entity to the transport service.
SNMP PDUs which had badValue error-status	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue'.

Field	Description
SNMP PDUs which had genErr error-status	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr'.
SNMP PDUs which had noSuchName error-status	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName'.
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `tooBig'.
MIB objects retrieved successfully	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
MIB objects altered successfully	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
GetRequest-PDU accepted and processed	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
GetNextRequest-PDU accepted and processed	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
GetBulkRequest-PDU accepted and processed	The total number of SNMP Get-Bulk PDUs which have been accepted and processed by the SNMP protocol entity.
GetResponse-PDU accepted and processed	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.
SetRequest-PDU accepted and processed	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
Trap PDUs accepted and processed	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.
Alternate Response Class PDUs dropped silently	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.

Field	Description
Forwarded Confirmed Class PDUs dropped silently	The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDU (such as a Response-PDU) could be returned.

display snmp-agent sys-info

Syntax

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

View

Any view

Parameters

contact: Displays the contact information of the current device.

location: Displays the physical location of the current device.

version: Displays the version information about the SNMP running in the system.

Description

Use the **display snmp-agent sys-info** command to display the system SNMP information about the current device, including contact information, geographical location of the device, and the employed SNMP version.

This command displays all the system SNMP information if you execute it with no keyword specified.

The **display snmp-agent sys-info** command displays the related information configured using the **snmp-agent sys-info** command. For the detailed configuration, refer to the **snmp-agent sys-info** command.

By default, the contact information of A Switch 4200G is "3Com Corporation.", the geographical location is " Marlborough, MA 01752 USA", and the SNMP version employed is SNMPv3.

Examples

Display the system SNMP information about the device.

```
<Sysname> display snmp-agent sys-info
   The contact person for this managed node:
          3Com Corporation.

   The physical location of this node:
          Marlborough, MA 01752 USA

   SNMP version running in the system:
```

display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

Any view

Parameters

None

Description

Use the **display snmp-agent trap-list** command to display the modules that can generate traps and whether the sending of traps is enabled on the modules.

If a module contains multiple submodules, the trap function of the entire module is displayed as enabled as long as the trap function of any of the submodules is enabled.

Related commands: **snmp-agent trap enable**.

Examples

Display the modules that can generate traps and whether the trap function is enabled on the modules.

```
<Sysname> display snmp-agent trap-list

   configuration trap enable

   flash trap enable

   standard trap enable

   system trap enable


   Enable traps :4; Disable traps 0
```

In the above output information, **enable** indicates that traps are allowed to be generated on the module, and **disable** indicates that traps are not allowed to be generated on the module.

By default, the modules that can generate traps are allowed to generate traps. If you do not need traps of some modules, you can use the **undo snmp-agent trap enable** command to disable the trap function of the specific modules.

display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **username** *user-name* | **group** *group-name*]*

View

Any view

Parameters

engineid: Engine ID, a string of 10 to 64 hexadecimal digits.

user-name: SNMPv3 username, a string of 1 to 32 characters.

group-name: Name of an SNMP group, a string of 1 to 32 characters.

Description

Use the **display snmp-agent usm-user** command to display the information about a specific type of SNMPv3 users.

If you execute this command with no keyword specified, the information about all the SNMPv3 users is displayed, including username, group name, engine ID, storage type and user status.

SNMPv3 introduced the concepts of username and group. You can set the authentication and privacy functions. The former is used to authenticate the validity of the sending end of the packets, preventing access of illegal users; the latter is used to encrypt packets between the NMS and agent, preventing the packets from being intercepted. A more secure communication between SNMP NMS and SNMP agent can be ensured by configuring whether to perform authentication and privacy or not.

You can configure whether to perform authentication and privacy when you create an SNMPv3 group, and configure the specific algorithms and passwords for authentication and privacy when you create a user.

Examples

Display the information about all the SNMP users.

```
<Sysname> display snmp-agent usm-user
   User name: usm-user
   Group name: usm-group9-0
       Engine ID: 800007DB000FE20F12346877
       Storage-type: nonVolatile
       UserStatus: active
```

Table 1-4 display snmp-agent usm-user command output description

Field	Description
User name	SNMP username
Group name	The name of the SNMP group which the SNMP user belongs to
Engine ID	SNMP engine ID of the device
Storage-type	Storage type, which can be: • volatile: Information will be lost if the system is rebooted • nonVolatile: Information will not be lost if the system is rebooted • permanent: Modification is permitted, but deletion is forbidden • readOnly: Read only, that is, no modification, no deletion • other: Other storage types
UserStatus	SNMP user status

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Ethernet port view, interface view

Parameters

None

Description

Use the **enable snmp trap updown** command to enable the sending of port/interface linkUp/linkDown traps.

Use the **undo enable snmp trap updown** command to disable the sending of linkUp/linkDown traps.

By default, the sending of port/interface linkUp/linkDown traps is enabled.

Note that you need to enable the generation of port/interface linkUp/linkDown traps both on the port/interface and globally if you want a port/interface to generate port/interface linkUp/linkDown traps when the state of the port/interface changes.

To enable this function on a port/interface, use the **enable snmp trap updown** command; to enable this function globally, use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command. By default, both are enabled.

Examples

Enable the port GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to the NMS whose IP address is 10.1.1.1 using the community name **public**.

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

Parameters

None

Description

Use the **snmp-agent** command to enable the SNMP agent.

Use the **undo snmp-agent** command to disable the SNMP agent.

Execution of the **snmp-agent** command or any of the commands used to configure the SNMP agent, you can start the SNMP agent.

By default, the SNMP agent is disabled.

Examples

Start the SNMP agent.

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

Note

A Switch 4200G provides the following functions to prevent attacks through unused UDP ports.

- Starting the SNMP agent opens UDP port used by SNMP agents and the UDP port used by SNMP trap respectively.
- Shutting down the SNMP agent closes UDP ports used by SNMP agents and SNMP trap as well.

---

snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

Parameters

plain-password: The plain-text password to be encrypted, in the range 1 to 64 characters.

mode: Specifies the authentication algorithm used to encrypt a plain text password.

md5: Uses HMAC MD5 algorithm.

sha: Uses HMAC SHA algorithm, which is securer than MD5 algorithm.

local-engineid: Uses the local engine ID to calculate the key.

specified-engineid: Uses the specified engine ID to calculate the key.

engineid: A case-insensitive hexadecimal string used for key calculation. The system capitalizes the string. The length of the string must be an even number and in the range 10 to 64 characters.

Description

Use the **snmp-agent calculate-password** command to encrypt a plain-text password to generate a cipher-text one by using the specified encryption algorithm.

When creating an SNMPv3 user, if you specify an authentication or privacy password as in cipher text, you need to use this command to generate a cipher text password by using the specified algorithm, and copy the generated cipher text password to use.

The generated password is related to engine ID: password generated under an engine ID can only take effect on this engine ID.

Related commands: **snmp-agent usm-user v3**.

 **Note**

SNMP agent must be enabled for you to encrypt a plain-text password.

Examples

Use the local engine ID and the md5 algorithm to encrypt plain-text password **aaaa**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent calculate-password aaaa mode md5 local-engineid
The result of the password is: B02A2E48346E2CBFFCE809C99CF1F6C
```

snmp-agent community

Syntax

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

undo snmp-agent community *community-name*

View

System view

Parameters

read: Specifies that the community to be created has read-only permission to MIB objects. Communities of this type can only query MIBs for device information.

write: Specifies that the community to be created has read-write permission to MIB objects. Communities of this type are capable of configuring devices.

community-name: Name of the community to be created, a string of 1 to 32 characters.

acl-number: ID of the ACL to be applied to the community, in the range 2000 to 2999. Using basic ACL can restrict the source addresses of SNMP messages, namely, permitting or refusing the SNMP messages with specific source addresses, thus restricting access between the NMS and the agent.

view-name: MIB view name, a string of 1 to 32 characters.

Description

Use the **snmp-agent community** command to create an SNMP community. SNMPv1 and SNMPv2c use community name to restrict access rights. You can use this command to configure a community name and configure read or write access right and ACL.

Use the **undo snmp-agent community** command to remove an SNMP community.

Typically, “public” is used as a read community name, and “private” is used as a write community name. For the security purposes, you are recommended to configure another community name except these two.

Examples

Create an SNMP community named **comaccess**, which has read-only permission to MIB objects.

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

Create an SNMP community named **mgr**, which has read-write permission to MIB objects

```
[Sysname] snmp-agent community write mgr
```

Remove the community named **comaccess**.

```
[Sysname] undo snmp-agent community comaccess
```

snmp-agent group

Syntax

1) Version 1 and version 2c

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

2) Version 3

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

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

System view

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Name of the SNMP group to be created, a string of 1 to 32 characters.

authentication: Configures to authenticate but do not encrypt the packets.

privacy: Configures to authenticate and encrypt the packets.

read-view: Read-only view name, a string of 1 to 32 characters. The default value is ViewDefault.

write-view: Read-write view name, a string of 1 to 32 characters. By default, no write view is configured, namely, the NMS cannot perform the write operation on the MIB objects of the device.

notify-view: Notification view name in which traps can be sent, a string of 1 to 32 characters. By default, no notify view is configured, namely, the agent will not send traps to the NMS.

acl-number: ID of a basic ACL, in the range 2000 to 2999. Using basic ACL can restrict the source addresses of SNMP messages, namely, permitting or refusing the SNMP messages with specific source addresses, thus restricting access between the NMS and the agent.

Description

Use the **snmp-agent group** command to create an SNMP group, and set the security mode and corresponding SNMP view of the group.

Use the **undo snmp-agent group** command to remove an SNMP group.

For SNMPv3, group name and security mode (whether authentication and privacy are performed) can jointly define a group. Groups with the same group name but different security mode are different groups. For the details, see the following examples.

By default, the SNMP groups created using the **snmp-agent group v3** command do not authenticate or encrypt packets.

Related commands: **snmp-agent mib-view**, **snmp-agent usm-user**.

Examples

Create an SNMPv1 group named **v1group**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent group v1 v1group
```

Create an SNMPv3 group **v3group**, set the security mode to no authentication no privacy, and set the read view, write view and view in which traps can be sent to ICMP view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent group v3 v3group read-view icmp write-view icmp notify-view icmp
```

Create an SNMPv3 group **v3group**, set the security mode to authentication and privacy, and permit only access from the NMS whose IP address is 192.168.0.108 to the agent using ACL.

```
[Sysname] acl number 2001
[Sysname] rule 0 permit source 192.168.0.108 0
[Sysname] snmp-agent group v3 v3group privacy acl 2001
```

In this case, when you use the **display snmp-agent group** command to display group information, you can see that two groups with the name **v3group** are created, but their security modes are noAuthnoPriv and AuthPriv respectively.

```
<Sysname> display snmp-agent group
   Group name: v3group
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: icmp
       Notifyview : icmp
       Storage-type: icmp
```

```
Group name: v3group
    Security model: v3 AuthPriv
    Readview: ViewDefault
    Writeview: <no specified>
    Notifyview :<no specified>
    Storage-type: nonVolatile
    Acl:2001
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

View

System view

Parameters

engineid: Engine ID, an even number of hexadecimal characters, in the range 10 to 64.

Description

Use the **snmp-agent local-engineid** command to set an engine ID for the local SNMP entity.

Use the **undo snmp-agent local-engineid** command to restore the default engine ID.

By default, the engine ID of an SNMP entity is formed by appending the device information to the enterprise number. The device information can be determined according to the device, which can be an IP address, a MAC address, or a user-defined string comprising of hexadecimal digits.

The configurations with the **snmp-agent usm-user v3** and **snmp-agent calculate-password** commands are related to engine ID. If you modify the engine ID, the corresponding configurations are invalid for the new engine ID.

Examples

Set the local SNMP entity engine ID to **123456789A**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent local-engineid 123456789A
```

snmp-agent log

Syntax

snmp-agent log { **set-operation** | **get-operation** | **all** }

undo snmp-agent log { **set-operation** | **get-operation** | **all** }

View

System view

Parameters

set-operation: Logs the set operations.

get-operation: Logs the get operations.

all: Logs both the set operations and get operations.

Description

Use the **snmp-agent log** command to enable network management operation logging.

Use the **undo snmp-agent log** command to disable network management operation logging.

By default, network management operation logging is disabled.

After SNMP logging is enabled, when NMS performs specified operations on the SNMP agent, the SNMP agent records and then saves the information related to the operations into the information center of the device.

Note

- When SNMP logging is enabled on a device, SNMP logs are output to the information center of the device. With the output destinations of the information center set, the output destinations of SNMP logs will be decided.
- The severity level of SNMP logs is informational, that is, the logs are taken as general prompt information of the device. To view SNMP logs, you need to enable the information center to output system information with **informational** level.
- For detailed description on system information and information center, refer to the *Information Center Configuration* part in this manual.

Examples

Enable logging for both the get and the set operations performed on the NMS.

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

snmp-agent mib-view

Syntax

snmp-agent mib-view { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

View

System view

Parameters

included: Specifies that the MIB view includes this MIB subtree.

excluded: Specifies that the MIB view excludes this MIB subtree.

view-name: View name.

oid-tree: OID MIB subtree of a MIB subtree. It can be the ID of a node in OID MIB subtree (such as 1.4.5.3.1) or an OID (such as “system”).

mask *mask-value:* Mask of a MIB subtree, an even number of hexadecimal characters, in the range 2 to 32. An odd number of characters are invalid.

Description

Use **snmp-agent mib-view** command to create or update the information about a MIB view to limit the MIB objects the NMS can access.

Use the **undo snmp-agent mib-view** command to cancel the current setting.

Management Information Base (MIB) is a collection of all the managed objects. MIB view is a sub-set of MIB. You can bind a community name/username with a MIB view when configuring an agent, thus to control the MIB objects that NMS can access. You can configure the objects in the MIB view as excluded or included; excluded indicates that all the nodes on the subtree are excluded in the current MIB view, and included indicates that the current MIB includes all the nodes on the subtree.

By default, the view name is ViewDefault, which includes all the MIB objects under the ISO MIB subtree except snmpUsmMIB, snmpVacmMIB and snmpModules.18.

If you specify a mask value in hexadecimal number when creating a MIB view, each bit number of the mask value corresponds with each sub-OID of the MIB subtree OID, from left to right. In a binary mask value, 1 indicates exact matching, meaning the OID of the node to be accessed must be the same as the sub-OID at the corresponding position of the MIB subtree OID; 0 indicates fuzzy matching, meaning the OID of the node to be accessed is not necessarily the same as the sub-OID at the corresponding position of the MIB subtree OID.

Note the following when defining a MIB view with a mask:

- If the bit number of a mask value is more than the number of sub-OIDs of the MIB subtree OID, the bit number remains unchanged.
- If the bit number of a mask value is less than the number of sub-OIDs of the OID of a MIB subtree, the bit number is filled by 1(s) in a binary number by default.
- If no mask value is specified when you create a MIB view, the OID of the node to be accessed must be the same as the sub-OID at the corresponding position of the MIB subtree OID. The mask value is displayed as null when the system reads it.

You need to define the MIB view access right of the community name or group in the configuration of an SNMP community name or group name. For the configurations, refer to the **snmp-agent community** and **snmp-agent group** commands.

Examples

Create an SNMP MIB view with the name of **icmp**, and MIB subtree of 1.3.6.1.2.1.5 to configure MIB view for the NMS to display or configure **icmp**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent mib-view included icmp 1.3.6.1.2.1.5
```

Create a read community name with the name of **icmpread**, and a write community name with the name of **icmpwrite**. Specify the MIB view as the configured icmp MIB view, and the NMS using this community name to access the device can only display or configure **icmp** related configurations.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]snmp-agent community read icmpread mib-view icmp
[Sysname]snmp-agent community write icmpwrite mib-view icmp
```

Create an SNMP MIB view with the name of **view-a**, MIB subtree of 1.3.6.1.5.4.3.4 and subtree mask of FE. MIB nodes with the OID of **1.3.6.1.5.4.3.x** are included in this view, with **x** indicating any integer number.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent mib-view included view-a 1.3.6.1.5.4.3.4 mask FE
```

snmp-agent packet max-size

Syntax

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

undo snmp-agent packet max-size

View

System view

Parameters

byte-count: Maximum SNMP packet size (in bytes) to be set, ranging from 484 to 17,940.

Description

Use the **snmp-agent packet max-size** command to set the maximum SNMP packet size allowed by an agent.

Use **undo snmp-agent packet max-size** command to restore the default maximum SNMP packet size.

The configuration of the maximum SNMP packet size is to prevent giant packets being discarded due to existence of devices not supporting fragmentation on a routing path. Typically, the maximum size of a packet can keep the default value of 1500 bytes.

By default, the maximum SNMP packet size allowed by an agent is 1,500 bytes.

Examples

Set the maximum SNMP packet size allowed by the agent to 1,042 bytes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent packet max-size 1042
```

snmp-agent sys-info

Syntax

snmp-agent sys-info { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c | v3** }* **| all** } }

undo snmp-agent sys-info { **contact** [**location**] | **location** [**contact**] | **version** { { **v1** | **v2c** | **v3** }* |**all** } }

View

System view

Parameters

sys-contact: Contact information for system maintenance, a string of up to 200 characters.

sys-location: Geographical location of the device, a string of up to 200 characters.

version: Specifies the SNMP version to be employed.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

all: Specifies all the SNMP versions available, that is, SNMPv1, SNMPv2c, and SNMPv3.

Description

Use the **snmp-agent sys-info** command to set the system information, including geographical location of the switch, contact information for system maintenance, and the SNMP version employed by the switch.

Use the **undo snmp-agent sys-info location** command to restore the default contact information and geographical location, or stop the running of the corresponding SNMP version.

If the switch fails, you can contact the switch manufacturer according to the system information.

The SNMP versions of the device and the NMS must be consistent; otherwise data exchange cannot be completed.

The device processes the SNMP messages of the corresponding SNMP version when the SNMP version is enabled on the device. If only SNMPv1 is enabled, while the device receives SNMPv2c messages, the messages will be discarded; if only SNMPv2c is enabled, the device discards the received SNMPv1 messages.

Multiple SNMP versions can be running the on the device at the same time to allow access of different NMSs.

By default, the contact information of a Switch 4200G is " 3Com Corporation.", the geographical location is " Marlborough, MA 01752 USA", and the SNMP version employed is SNMPv3.

You can use the **display snmp-agent sys-info** command to display the current SNMP system information.

Examples

Specify the contact information for system maintenance as **Dial System Operator # 1234**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent sys-info contact Dial System Operator # 1234
```

snmp-agent target-host

Syntax

snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host *ip-address* **securityname** *security-string*

View

System view

Parameters

trap: Enables the host to receive SNMP traps.

address: Specifies the destination for the SNMP traps.

udp-domain: Specifies to use UDP to communicate with the target host.

ip-address: The IPv4 address of the host that is to receive the traps.

port-number: Number of the UDP port that is to receive the traps, in the range 1 to 65,535.

params: Specifies SNMP target host information to be used in the generation of SNMP traps.

security-string: SNMPv1/SNMPv2c community name or SNMPv3 username, a string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

authentication: Configures to authenticate the packets without encryption.

privacy: Configures to authenticate and encrypt the packets.

Description

Use **snmp-agent target-host** command to set a destination host to receive the SNMP traps generated by the local device.

Use **undo snmp-agent target-host** command to cancel the current setting.

You can configure multiple destination hosts to receive traps with the command as needed.

To enable a device to send SNMP traps, the **snmp-agent target-host** command need to be coupled with a command among the **snmp-agent trap enable** command and the **enable snmp trap updown** command.

1) Use the **snmp-agent trap enable** or **enable snmp trap updown** command to specify the types of the SNMP traps a device can send (by default, a device can send all types of SNMP traps).
2) Use the **snmp-agent target-host** command to set the address of the destination for the SNMP traps.

Related commands: **snmp-agent trap enable**, **snmp-agent trap source**, and **snmp-agent trap life**.

Examples

Enable sending SNMP traps to 10.1.1.1, and set the community name to **public**.

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

```
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

undo snmp-agent trap enable [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

View

System view

Parameters

configuration: Specifies to send configuration traps.

flash: Specifies to send Flash traps.

standard: Specifies to send SNMP standard notification or traps.

authentication: Specifies to send SNMP authentication failure traps in cases of authentication failures.

coldstart: Specifies to send SNMP cold start traps when the device is rebooted.

linkdown: Specifies to send SNMP linkDown traps when a port becomes down.

linkup: Specifies to send SNMP linkUp traps when a port becomes up.

warmstart: Specifies to send SNMP warm start traps when SNMP is newly launched.

system: Specifies to send SYS-MAN-MIB (proprietary MIB) traps.

Description

Use the **snmp-agent trap enable** command to enable a device to send SNMP traps that are of specified types.

Use the **undo snmp-agent trap enable** command to disable a device from sending SNMP traps that are of specified types.

By default, a device sends all types of SNMP traps.

The **snmp-agent trap enable** command need to be coupled with the **snmp-agent target-host** command. The **snmp-agent target-host** command specifies the destination hosts for SNMP traps. At least one destination host is required for SNMP traps.

Examples

Enable sending of SNMP authentication failure traps, with the destination IP address being 10.1.1.1 and the community name being **public**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent trap enable standard authentication
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

snmp-agent trap ifmib

Syntax

snmp-agent trap ifmib link extended

undo snmp-agent trap ifmib link extended

View

System view

Parameters

None

Description

Use the **snmp-agent trap ifmib link extended** command to configure the extended trap. “Interface description” and “interface type” are added into the extended linkUp/linkDown trap.

Use the **undo snmp-agent trap ifmib link extended** command to restore the default setting.

By default, the linkUp/linkDown trap uses the standard format defined in IF-MIB (refer to RFC 1213 for detail). In this case, no MIB object name is added after the OID field of the MIB object.

Examples

Before the configuration of the extended trap function, the trap information is as follows when a link is down:

```
#Apr  2 05:53:15:883 2000 3Com L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.3(linkDown): portIndex is 4227634, ifAdminStatus is 2, ifOperStatus
is 2
#Apr  2 05:53:16:094 2000 3Com IFNET/5/TRAP:- 1 -1.3.6.1.6.3.1.1.5.3(linkDown) Interface 31
is Down
```

Configure the extended linkUp/linkDown trap format to make traps include the interface description and interface type information.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent trap ifmib link extended
```

After the configuration of the extended trap function, the trap information is as follows when a link is down:

```
#Apr  2 05:55:00:642 2000 3Com L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.3(linkDown): portIndex is 4227634, ifAdminStatus is 2, ifOperStatus
is 2,ifDescr='GigabitEthernet1/0/2', ifType=6
#Apr  2 05:55:00:893 2000 3Com IFNET/5/TRAP:- 1 -1.3.6.1.6.3.1.1.5.3(linkDown) Interface 31
is Down. ifAdminStatus=1, ifOperStatus=2, ifDescr='Vlan-interface1',ifType=136
```

The above output indicates that the interface description and interface type information is added into the traps, thus facilitating fault location.

snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

View

System view

Parameters

seconds: SNMP trap aging time (in seconds) to be set, ranging from 1 to 2,592,000.

Description

Use the **snmp-agent trap life** command to set the SNMP trap aging time. SNMP traps exceeding the aging time will be discarded.

Use the **undo snmp-agent trap life** command to restore the default SNMP trap aging time.

By default, the SNMP trap aging time is 120 seconds.

The system discards the traps that timed out and not sent in the SNMP trap queue.

Related commands: **snmp-agent trap enable**, **snmp-agent target-host**.

Examples

Set the SNMP trap aging time to 60 seconds.

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

Parameters

size: The maximum number of traps that can be stored in the queue, an integer ranging from 1 to 1,000.

Description

Use the **snmp-agent trap queue-size** command to set the length of the queue of the SNMP traps to be sent to the destination.

Use the **undo snmp-agent trap queue-size** command to restore the default queue length.

By default, an SNMP trap queue can contain up to 100 SNMP traps.

After a trap is generated, it will enter the trap queue to be sent. The length of a trap queue decides the maximum number of traps in the queue. When a trap queue reaches the configured length, the newly generated traps will enter the queue, and the traps generated the earliest will be discarded.

Related commands: **snmp-agent trap enable**, **snmp-agent target-host**, and **snmp-agent trap life**.

Examples

Set the SNMP trap queue length to 200.

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

Parameters

interface-type interface-number: Interface type and interface number. The source IP address of the trap is the IP address of this interface.

Description

Use the **snmp-agent trap source** command to configure the source address for the SNMP traps sent.

Use the **undo snmp-agent trap source** command to cancel the configuration.

By default, the outbound interface is determined by SNMP and the IP address of this interface is used as the source IP address of the traps.

After the command is executed, the system uses the primary IP address of the specified interface as the source IP address of the traps sent. Thus on the NMS you can use the IP address to uniquely identify the agent.

For example, although the agent uses different outbound interfaces to send traps, the NMS can still use the IP address to filter all the traps that the agent sends.

You can configure this command to track a specific event by the source addresses of SNMP traps.

Note

Before configuring an interface as the source interface for the SNMP traps sent, make sure the interface is assigned an IP address.

Related commands: **snmp-agent trap enable**, **snmp-agent target-host**.

Examples

Configure VLAN-interface 1 as the source interface for the SNMP traps sent.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] snmp-agent trap source Vlan-interface 1
```

snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

View

System view

Parameters

v1: Creates an SNMPv1 user.

v2c: Creates an SNMPv2c user.

v3: Specifies to use SNMPv3 security mode.

user-name: Name of the user to be added, a string of 1 to 32 characters.

group-name: Name of the group corresponding to the user, a string of 1 to 32 characters.

acl-number: ID of a basic ACL, in the range 2000 to 2999. Using basic ACL can restrict the source addresses of SNMP messages, namely, permitting or refusing the SNMP messages with specific source addresses, thus restricting access between the NMS and the agent.

Description

Use the **snmp-agent usm-user** { **v1** | **v2c** } command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user** { **v1** | **v2c** } command to remove a user from an SNMP group.

This command is applicable to SNMPv1 and SNMPv2c, and is equal to using the **snmp-agent community** command to create a community.

As the SNMP protocol defines, in the networking of SNMPv1 and SNMPv2c, community name is used for authentication between NMS and agent, and in the networking of SNMPv3, username is used for authentication. If you want to configure a username and use the username for authentication, the device supports SNMPv1 and SNMPv2c users. Creating an SNMPv1 or SNMPv2c user is equal to adding a new community name. If you fill the newly created username into the community name field of the NMS, the NMS can establish a connection with the SNMP.

To make the configured user take effect, you must create a group first.

Related commands: **snmp-agent group**, **snmp-agent community**, and **snmp-agent local-engineid**.

Examples

Create a group named **readCom** and an SNMPv2c user **userv2c**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
```

```
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

Specify the SNMP version of the NMS as **SNMPv2c**, fill the write community name field with **userv2c**. Then the NMS can access the agent.

Create an SNMPv2c user **userv2c** in group **readCom**, permitting only the NMS with an IP address 1.1.1.1 to access the agent, and denying the access of other NMSs.

```
<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
```

Specify the SNMP version of the NMS with an IP address 1.1.1.1 as **SNMPv2c**, fill the write community name field with **userv2c**. Then the NMS can access the agent.

snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **des56** | **aes128** } *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **engineid** *engineid-string* }

View

System view

Parameters

user-name: Username, a string of 1 to 32 characters.

group-name: Name of the group corresponding to the user, a string of 1 to 32 characters.

cipher: Specifies the authentication password (*auth-password*) or encryption password (*priv-password*) to be in cipher text. The cipher text password can be calculated using the **snmp-agent calculate-password** command.

authentication-mode: Specifies the security mode as authentication required. If you do not specify this keyword, neither authentication nor encryption is performed.

md5: Uses HMAC MD5 algorithm for authentication.

sha: Uses HMAC SHA algorithm for authentication, which is securer than MD5.

auth-password: Authentication password, a string of 1 to 64 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

privacy: Specifies the security mode as encrypted.

des56: Specifies the encryption protocol as Data Encryption Standard (DES).

aes128: Specifies the encryption protocol as Advanced Encryption Standard (AES), which is securer than DES.

priv-password: Encryption password, a string of 1 to 64 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

acl-number: Binds a user with an ACL, where *acl-number* represents ACL number, in the range 2000 to 2999. Using ACLs can restrict the source addresses of SNMP messages, namely, permitting or refusing the SNMP messages with specific source addresses, thus restricting access between the NMS and the agent.

local: Specifies a local entity user.

engineid-string: Engine ID associated with the user, an even number of hexadecimal characters, in the range 10 to 64.

Description

Use the **snmp-agent usm-user** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user** command to remove a user from an SNMP group.

This command is applicable to SNMPv3. If the agent and the NMS communicate using SNMPv3 messages, you need to create an SNMPv3 user first.

To make the configured user take effect, you need to create a group first. You can configure whether to perform authentication or privacy when you create a group, and configure the algorithm and password for authentication or privacy when you create a user.

An SNMPv3 user is related the engine ID: if you change the engine ID after configuring a user, the user corresponding to the original engine ID becomes invalid.

Note that:

- If the password is in cipher text, the *pri-password* argument can be obtained by the **snmp-agent calculate-password** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command, ensure that the same authentication algorithm is specified for the two commands and the local engine ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity engine ID specified in the **snmp-agent calculate-password** command.
- If you use the command repeatedly to configure the same user (namely, with the same username), the last configuration takes effect.
- You must enter a plain text password when the NMS accesses the device. Therefore, when you create a user, you need to memorize the username and the corresponding plain text password.

Related commands: **snmp-agent group**, **snmp-agent community**, **snmp-agent local-engineid**.

Examples

Add a user named **testUser** to the SNMPv3 group named **testGroup**. Set the security mode to authentication without privacy, the authentication algorithm to **md5**, and authentication password **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
```

On the NMS, set the version to **SNMPv3**, the username to **testUser**, the authentication algorithm to **MD5**, and the authentication password to **authkey**, and establish a connection with the device. Then the NMS can access the MIB objects in the view **ViewDefault** on the device.

Add a user named **testUser** to the SNMPv3 group named **testGroup**. Set the security mode to authentication with privacy, the authentication algorithm to **md5**, the privacy algorithm to **des56**, the plain text authentication password to **authkey**, the plain text privacy password to **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
```

On the NMS, set the version to **SNMPv3**, the username to **testUser**, the authentication algorithm to **MD5**, the authentication password to **authkey**, the privacy algorithm to **DES**, and the privacy password to **prikey**, and establish a connection with the device. Then the NMS can access the MIB objects in the view **ViewDefault** on the device.

Add a user named **testUser** to the SNMPv3 group named **testGroup** in cipher mode (namely, the authentication and privacy passwords should be in cipher text). Set the security mode to authentication with privacy, the authentication algorithm to **md5**, the privacy algorithm to **des56**, the authentication password to **authkey**, and the cipher text privacy password to **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
```

On the NMS, set the version to **SNMPv3**, the username to **testUser**, the authentication algorithm to **MD5**, the authentication password to **authkey**, the privacy algorithm to **DES**, and the privacy password to **prikey**, and establish a connection with the device. Then the NMS can access the MIB objects in the view **ViewDefault** on the device.

2 RMON Configuration Commands

RMON Configuration Commands

display rmon alarm

Syntax

display rmon alarm [*entry-number*]

View

Any view

Parameters

entry-number: Alarm entry index, in the range 1 to 65535.

Description

Use the **display rmon alarm** command to display the configuration of a specified alarm entry or all the alarm entries. The configuration information includes: sampling type, sampled node, sampling interval, rising and falling thresholds that trigger alarms, the condition under which an alarm is triggered, and the last sampled value.

Related commands: **rmon alarm**.

Examples

Display the configuration of all the alarm entries.

```
<Sysname> display rmon alarm
Alarm table 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     : 20(sec)
  Rising threshold      : 100(linked with event 1)
  Falling threshold     : 10(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 5510006
```

Table 2-1 display rmon alarm command output description

Field	Description
Alarm table	Index of an entry in the alarm entry
user1	Entry owner: user1
Valid	The alarm entry identified by the index is valid.
Samples type	Sampling type, which can be absolute or delta
Variable formula	The sampled node

Field	Description
Sampling interval	Sampling interval, in seconds. The system performs absolute or delta sampling on the sampled node at this interval.
Rising threshold	Rising threshold. When the sampled value equals or exceeds the rising threshold, an alarm is triggered.
Falling threshold	Falling threshold. When the sampled value equals or falls under the falling threshold, an alarm is triggered.
When startup enables	The condition under which an alarm is triggered, which can be: • risingOrFallingAlarm: An alarm is triggered when the rising or falling threshold is reached. • risingAlarm: An alarm is triggered when the rising threshold is reached. • FallingAlarm: An alarm is triggered when the falling threshold is reached.
Latest value	The value of the latest sample

display rmon event

Syntax

display rmon event [*event-entry*]

View

Any view

Parameters

event-entry: RMON event entry index, in the range 1 to 65535. If you do not specify the *event-entry* argument, the configuration of all the RMON event entries is displayed.

Description

Use the **display rmon event** command to display the configuration of a specified RMON event entry.

RMON event information includes the following:

- Event entry index
- Event entry owner
- Event description
- The action triggered by the event (log or alarm messages)
- The time (in seconds) when the latest event is triggered (in terms of the time elapsed since the system is started/initialized).

Related commands: **rmon event**.

Examples

Display the configuration of all the RMON event entries.

```
<Sysname> display rmon event
```

```
Event table 1 owned by user1 is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 2-2 display rmon event command output description

Field	Description
Event table	Index of an entry in the RMON event table
VALID	The status of the entry identified by the index is valid.
Description	RMON event description
Will cause log-trap when triggered	The event triggers logging and an alarm trap.
last triggered at	Time when the latest event is triggered

display rmon eventlog

Syntax

display rmon eventlog [*event-entry*]

View

Any view

Parameters

event-entry: RMON event entry index, in the range 1 to 65,535. If you do not specify the *event-entry* argument, the logs of all the RMON events are displayed.

Description

Use the **display rmon eventlog** command to display the log of an RMON event.

On creating an RMON event, you can configure to record the event information into the logbuffer when an event is triggered, thus facilitating displaying of the information. The recorded information includes:

- RMON event entry Index
- Current RMON event entry status
- The time (in seconds) when an event log is generated (in terms of the time elapsed since the system is started or initialized)
- RMON event description.

Examples

Display the log generated by the event entry numbered 1.

```
<Sysname> display rmon eventlog 1
Event table 1 owned by user1 is VALID.
Generates eventLog 1.1 at 0days 00h:01m:39s.
Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
Generates eventLog 1.2 at 0days 00h:02m:27s.
Description: The alarm formula defined in private alarm table 1,
```

```
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

Table 2-3 display rmon eventlog command output description

Field	Description
Event table	Index of an entry in the RMON event table
VALID	The status of the entry identified by the index is valid.
Generates eventLog 1.1 at 0days 00h:02m:27s	Time when the event is triggered. The event can be triggered for multiple times. 1.1 indicates the time when event 1 is first triggered.
Description	Description of the RMON event log

The above output indicates that two logs are generated due to event 1:

- Log 1.1 is generated from alarm entry 1, because the sampled value (0) of the alarm entry is lower than the falling threshold (100). The sampling type is **absolute**.
- Log 1.1 is generated from prialarm entry 1, because the sampled value (0) of the prialarm entry is lower than the falling threshold (100). The sampling type is **absolute**.

display rmon history

Syntax

display rmon history [*interface-type interface-number* | **unit** *unit-number*]

View

Any view

Parameters

interface-type: Interface type.

interface-number: Interface number.

unit *unit-number*: Specifies a unit number.

Description

Use the **display rmon history** command to display the RMON history information about a specified port. The information about the latest sample, including bandwidth utilization, the number of errors, the total number of packets, and so on, is also displayed.

After a history entry is created on a port, the system collects statistics of the port at a certain interval, and saves the information in the etherHistoryEntry table. You can use the command to display the records saved in the table.

If you do not provide the *interface-type interface-number* or *unit-number* argument, this command displays the RMON history information about all the ports/units.

Related commands: **rmon history**.

Examples

Display the RMON history information about GigabitEthernet 1/0/1.

```
<Sysname> display rmon history GigabitEthernet 1/0/1
```

```
History control entry 1 owned by user1 is VALID
  Samples interface     : GigabitEthernet1/0/1<ifIndex.4227625>
  Sampling interval     : 5(sec) with 10 buckets max
  Latest sampled values :
  Dropevents        : 0         , octets               : 10035
  packets           : 64        , broadcast packets    : 35
  multicast packets : 8         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets     : 0
  fragments         : 0         , jabbers              : 0
  collisions        : 0         , utilization          : 0
```

Table 2-4 display rmon history command output description

Field	Description
History control entry	Index of an entry in the history control table
VALID	The status of the entry identified by the index is valid.
Samples interface	Interface on which statistics are collected
Sampling interval	Statistics interval in seconds. The system collects statistics of the port at this interval.
buckets	Number of the records in the history control table
Latest sampled values	Latest sampled values
dropevents	Number of the packet-dropping events
octets	Number of the received/transmitted bytes during sampling duration
packets	Number of the received/transmitted packets during sampling duration
broadcastpackets	Number of the broadcast packets
multicastpackets	Number of the multicast packets
CRC alignment errors	Number of the packet with CRC errors
undersize packets	Number of the undersize packets
oversize packets	Number of the oversize packets
fragments	Number of the undersize packets with CRC errors
jabbers	Number of the oversize packets with CRC errors
collisions	Number of the packets that cause collisions
utilization	Bandwidth utilization

display rmon prialarm

Syntax

display rmon prialarm [*prialarm-entry-number*]

View

Any view

Parameters

prialarm-entry-number: Extended alarm entry Index, in the range 1 to 65,535.

Description

Use the **display rmon prialarm** command to display the configuration of an RMON extended alarm entry. If you do not specify the *prialarm-entry-number* argument, the configuration of all the extended alarm entries is displayed.

The information in an extended alarm entry includes: sampling type, variable formula of the sampled node, sampling interval, rising and falling thresholds that trigger an alarm, the condition under which an alarm is triggered, and the last sampled value.

Related commands: **rmon prialarm**.

Examples

Display the configuration of all the extended RMON alarm entries.

```
<Sysname> display rmon prialarm
Prialarm table 1 owned by user1 is VALID.
  Samples type          : absolute
  Variable formula      : ((.1.3.6.1.2.1.16.1.1.1.4.1)*100)
  Description           :
  Sampling interval     : 10(sec)
  Rising threshold      : 10000(linked with event 1)
  Falling threshold     : 2000(linked with event 1)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value          : 0
```

Table 2-5 display rmon prialarm command output description

Field	Description
Prialarm table	Index of an entry in the extended alarm table
owned by user1	Entry owner: user 1
VALID	The alarm entry identified by the index is valid.
Samples type	Sampling type: absolute or delta
Variable formula	Variable formula of the sampled node
Description	Description
Sampling interval	Sampling interval in seconds. The system collects statistics of the port at this interval.
Rising threshold	Rising threshold. When the sampled value equals or exceeds the rising threshold, an alarm is triggered.
Falling threshold	Falling threshold. When the sampled value equals or falls under the falling threshold, an alarm is triggered.

Field	Description
Linked with event	Event index corresponding to an alarm
When startup enables: risingOrFallingAlarm	The condition under which an alarm is triggered, which can be: • risingOrFallingAlarm: An alarm is triggered when the rising or falling threshold is reached. • risingAlarm: An alarm is triggered when the rising threshold is reached. • FallingAlarm: An alarm is triggered when the falling threshold is reached.
This entry will exist: forever	Existing period. This entry can exist forever or exist in the specified cycle
Latest value	The value of the latest sample

display rmon statistics

Syntax

display rmon statistics [*interface-type interface-number* | **unit** *unit-number*]

View

Any view

Parameters

interface-type: Interface type.

interface-number: Interface number.

unit *unit-number*: Specifies a unit number.

Description

Use the **display rmon statistics** command to display the RMON statistics on a specified port or a specified unit. If you do not specify the port or the unit, this command displays the RMON statistics on all the ports or units.

The information displayed includes the number of:

- Collisions
- Packets with CRC errors
- Undersize/Oversize packets
- Broadcast/multicast packets
- Received bytes
- Received packets

Related commands: **rmon statistics**.

Examples

Display the RMON statistics on GigabitEthernet 1/0/1 port.

```
<Sysname> display rmon statistics GigabitEthernet 1/0/1
Statistics entry 1 owned by user1-rmon is VALID.
```

```
Interface : GigabitEthernet1/0/1<ifIndex.4227625>
etherStatsOctets         : 30561     , etherStatsPkts          : 217
etherStatsBroadcastPkts  : 102       , etherStatsMulticastPkts : 25
etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
etherStatsFragments      : 0         , etherStatsJabbers       : 0
etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
etherStatsDropEvents (insufficient resources): 0
Packets received according to length:
64     : 177       ,  65-127  : 27        ,  128-255  : 2
256-511: 0         ,  512-1023: 0         ,  1024-1518: 11
```

Table 2-6 display rmon statistics command output description

Field	Description
Statistics entry	Index of the statistics information entry
VALID	The statistics table is valid.
Interface	Interface which the statistics is on
etherStatsOctets	Number of bytes received
etherStatsPkts	Number of the packets received
etherStatsBroadcastPkts	Number of broadcast packets received
etherStatsMulticastPkts	Number of multicast packets received
etherStatsUndersizePkts	Number of undersize packets received
etherStatsOversizePkts	Number of oversize packets received
etherStatsFragments	Number of undersize packets received with CRC errors
etherStatsJabbers	Number of oversize packets received with CRC errors
etherStatsCRCAlignErrors	Number of packets received with CRC errors
etherStatsCollisions	Number of the received packets that cause collisions
etherStatsDropEvents	Event about dropping packets
Packets received according to length	Number of the received packets that are of different lengths

rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

View

System view

Parameters

entry-number: Index of the alarm entry to be added/removed, in the range 1 to 65535.

alarm-variable: Alarm variable, a string comprising 1 to 256 characters in dotted node OID format (such as 1.3.6.1.2.1.2.1.10.1). Only the variables that can be resolved to ASN.1 INTEGER data type (that is, INTEGER, Counter, Gauge, or TimeTicks) can be used as alarm variables.

sampling-time: Sampling interval (in seconds), in the range 5 to 65,535.

delta: Specifies to sample increments (that is, the current increment with regard to the latest sample)

absolute: Specifies to sample absolute values.

rising_threshold *threshold-value1*: Specifies the rising threshold. The *threshold-value1* argument ranges from 0 to 2,147,483,647.

event-entry1: Index of the event entry corresponding to the rising threshold, in the range of 0 to 65535.

falling_threshold *threshold-value2*: Specifies the falling threshold. The *threshold-value2* argument ranges from 0 to 2,147,483,647.

event-entry2: Index of the event entry corresponding to the falling threshold, in the range 0 to 65535.

owner *text*: Specifies the owner of the entry, a string of 1 to 127 characters.

Description

Use the **rmon alarm** command to add an alarm entry to the alarm table. If you do not specify the **owner** *text* keyword/argument combination, the owner of the entry is displayed as “null”.

Use the **undo rmon alarm** command to remove an alarm entry from the alarm table.

You can use the **rmon alarm** command to define an alarm entry so that a specific alarm event can be triggered under specific circumstances. The act (such as logging and sending traps to NMS) taken after an alarm event occurs is determined by the corresponding alarm entry.

Note

Before adding an alarm entry, make sure the events to be referenced in the alarm entry exist. Refer to the **rmon event** command for related information.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sample the defined alarm variables (*alarm-variable*) once in each specified period, which is specified by the *sampling-time* argument.
- Comparing the sampled value with the set thresholds and performing the corresponding operations, as described in Table 2-7.

Table 2-7 Sample value and the corresponding operation

Comparison	Operation
The sample value is larger than or equal to the set upper threshold (*threshold-value1*)	Triggering the event identified by the *event-entry1* argument

Comparison	Operation
The sample value is smaller than the set lower threshold (*threshold-value2*)	Triggering the event identified by the *event-entry2* argument

Note

- Before adding an alarm entry, you need to use the **rmon event** command to define the events to be referenced by the alarm entry.
- Make sure the node to be monitored exists before executing the **rmon alarm** command.

Examples

Add the alarm entry numbered 1 as follows:

- The node to be monitored: 1.3.6.1.2.1.16.1.1.1.4.1
- Sampling interval: 10 seconds
- Upper threshold: 50
- The *event-entry1* argument identifies event 1.
- Lower threshold: 5
- The *event-entry2* argument identifies event 2
- Owner: user1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising_threshold 50 1
falling_threshold 5 2 owner user1
```

Remove the alarm entry numbered 15 from the alarm table.

```
[Sysname] undo rmon alarm 15
```

rmon event

Syntax

rmon event *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]

undo rmon event *event-entry*

View

System view

Parameters

event-entry: Event entry index, in the range of 1 to 65535.

description *string*: Specifies the event description, a string of 1 to 127 characters.

log: Logs events.

trap: Sends traps to the NMS.

trap-community: Community name of the NMS that receives the traps, a string of 1 to 127 characters.

log-**trap**: Logs the event and sends traps to the NMS.

log-trapcommunity: Community name of the NMS that receives the traps, a character string of 1 to 127 characters.

none: Specifies that the event triggers no action.

owner *text*: Specifies the owner of the event entry, a string of 1 to 127 characters.

Description

Use the **rmon event** command to add an entry to the event table. If you do not specify the **owner** *text* keyword/argument combination, the owner of the entry is displayed as “null”.

Use the **undo rmon event** command to remove an entry from the event table.

When adding an event entry to an event table, you need to specify the event index. You need also to specify the corresponding actions, including logging the event, sending traps to the NMS, and the both, for the network device to perform corresponding operation when an alarm referencing the event is triggered.

Examples

Add the event entry numbered 10 to the event table and configure it to be a log event.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rmon event 10 log
```

rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

View

Ethernet port view

Parameters

entry-number: History entry index, in the range of 1 to 65535.

buckets *number*: Specifies the size of the history table that corresponds to the entry, in the range 1 to 65535.

interval *sampling-interval*: Specifies the sampling interval (in seconds). The *sampling-interval* argument ranges from 5 to 3600.

owner *text*: Specifies the owner of the entry, a string of 1 to 127 characters.

Description

Use the **rmon history** command to add an entry to the history control table. If you do not specify the **owner** *text* keyword/argument combination, the owner of the entry is displayed as “null”.

Use the **undo rmon history** command to remove an entry from the history control table.

You can use the **rmon history** command to sample a specific port. You can also set the sampling interval and the number of the samples that can be saved. After you execute this command, the RMON system samples the port periodically and stores the samples for later retrieval. The sampled information includes utilization, the number of errors, and total number of packets.

You can use the **display rmon history** command to display the statistics of the history control table.

Examples

Create the history control entry numbered 1 for GigabitEthernet 1/0/1, with the table size being 10, the sampling interval being 5 seconds, and the owner being **user1**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]rmon history 1 buckets 10 interval 5 owner user1
```

Remove the history control entry numbered 15.

```
[Sysname-GigabitEthernet1/0/1] undo rmon history 15
```

rmon prialarm

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **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

Parameters

entry-number: Extended alarm entry index, in the range 1 to 65535.

prialarm-formula: Expression used to perform operations on the alarm variables, a string of 1 to 256 characters. The alarm variables in the expression must be represented by OIDs, for example, (.1.3.6.1.2.1.2.1.10.1)*8. The operations available are addition, subtraction, multiplication and division operations. The operation results are rounded to values that are of long integer type. To prevent invalid operation results, make sure the operation results of each step are valid long integers.

prialarm-des: Alarm description, a string of 1 to 128 characters.

sampling-timer: Sampling interval (in seconds), in the range 10 to 65535.

delta | **absolute** | **changeratio**: Specifies the sample type.

threshold-value1: Upper threshold, in the range 0 to 2147483647.

event-entry1: Index of the event entry that corresponds to the rising threshold, in the range 0 to 65535.

threshold-value2: Lower threshold, in the range 0 to 2147483647.

event-entry2: Index of the event entry that corresponds to the falling threshold, in the range 0 to 65535.

forever: Specifies the corresponding RMON alarm instance is valid permanently.

cycle: Specifies the corresponding RMON alarm instance is valid periodically.

cycle-period: Life time (in seconds) of the RMON alarm instance, in the range 0 to 2147483647.

owner *text*: Specifies the owner of the alarm entry, a string of 1 to 127 characters.

Description

Use the **rmon prialarm** command to create an extended entry in an extended RMON alarm table. If you do not specify the **owner** *text* keyword/argument combination, the owner of the entry is displayed as "null".

Use the **undo rmon prialarm** command to remove an extended alarm entry.

Note

- Before adding an extended alarm entry, you need to use the **rmon event** command to define the events to be referenced by the entry.
- Make sure the node to be monitored exists before executing the **rmon event** command.
- You can define up to 50 extended alarm entries.

With an extended alarm entry defined in an extended alarm group, the device performs the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expression (*prialarm-formula*) once in each period specified by the *sampling-timer* argument.
- Performing operations on the sampled values according to the defined extended alarm expression (*prialarm-formula*)
- Comparing the operation result with the set thresholds and perform corresponding operations, as described in Table 2-8.

Table 2-8 Operation result and corresponding operation

Comparison	Operation
The operation result is larger than or equal to the set upper threshold (*threshold-value1*)	Triggering the event identified by the *event-entry1* argument
The operation result is smaller than or equal to the set lower threshold (*threshold-value2*)	Triggering the event identified by the *event-entry2* argument

Examples

Add the extended alarm entry numbered 2 as follows:

- Perform operations on the corresponding alarm variables using the expression ((1.3.6.1.2.1.16.1.1.1.4.1)*100).
- Sampling interval: 10 seconds
- Rising threshold: 50

- Falling threshold: 5
- Event 1 is triggered when the change ratio is larger than the rising threshold.
- Event 2 is triggered when the change ratio is less than the falling threshold.
- The alarm entry is valid forever.
- Entry owner: user1

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 2 ((.1.3.6.1.2.1.16.1.1.1.4.1)*100) test 10 changeratio
rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1
```

Remove the extended alarm entry numbered 2 from the extended alarm table.

```
[Sysname] undo rmon prialarm 2
```

rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

View

Ethernet port view

Parameters

entry-number: Statistics entry Index, in the range 1 to 65535.

owner *text*: Specifies the owner of the entry, a string of 1 to 127 characters.

Description

Use the **rmon statistics** command to add an entry to the statistics table. If you do not specify the **owner** *text* keyword/argument combination, the owner of the entry is displayed as “null”.

Use the **undo rmon statistics** command to remove an entry from the statistics table.

The RMON statistics management function is used to take statistics of the usage of the monitored ports and errors occurred on them. The statistics includes the number of the following items:

- Collisions
- Packets with CRC errors
- Undersize/Oversize packets
- Broadcast/Multicast packets
- Received packets
- Received bytes

Note

For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry was already created for a given port, you will fail to create a statistics entry with a different index for the port.

You can use the **display rmon statistics** command to display the information about the statistics entry.

Examples

Add the statistics entry numbered 20 to take statistics of GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20
```

Table of Contents

1 IGMP Snooping Configuration Commands

IGMP Snooping Configuration Commands

display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

Any view

Parameters

None

Description

Use the **display igmp-snooping configuration** command to display IGMP Snooping configuration information.

If IGMP Snooping is disabled on this switch, this command displays a message showing that IGMP Snooping is not enabled.

With IGMP Snooping enabled, this command displays the following information:

- IGMP Snooping status
- aging time of the router port
- maximum response time in IGMP queries
- aging time of multicast member ports
- non-flooding feature status

Related commands: **igmp-snooping**, **igmp-snooping router-aging-time**, **igmp-snooping max-response-time**, **igmp-snooping host-aging-time**, **igmp-snooping nonflooding-enable**.

Examples

Display IGMP Snooping configuration information on the switch.

```
<Sysname> display igmp-snooping configuration
 Enable IGMP-Snooping.
   The router port timeout is 105 second(s).
   The max response timeout is 10 second(s).
   The host port timeout is 260 second(s).
   Enable IGMP-Snooping Non-Flooding.
```

The above-mentioned information shows: IGMP Snooping is enabled, the aging time of the router port is 105 seconds, the maximum response time in IGMP queries is 10 seconds, the aging time of multicast member ports is 260 seconds, and the IGMP Snooping non-flooding feature is enabled.

display igmp-snooping group

Syntax

display igmp-snooping group [**vlan** *vlan-id*]

View

Any view

Parameters

vlan *vlan-id*: Specifies the VLAN in which the multicast group information is to be displayed, where *vlan-id* ranges from 1 to 4094. If you do not specify a VLAN, this command displays the multicast group information of all VLANs.

Description

Use the **display igmp-snooping group** command to display the IGMP Snooping multicast group information.

Related commands: **igmp-snooping**, **igmp host-join**, **multicast static-group vlan**, **multicast static-group interface**, **multicast static-group vlan**, **multicast static-router-port**, **multicast static-router-port vlan**

Examples

Display the information about the multicast groups in all VLANs.

```
<Sysname> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).
  Vlan(id):99.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static Router port(s):
                    GigabitEthernet1/0/11
    Dynamic Router port(s):
                    GigabitEthernet1/0/22
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:228.0.0.0
        Static host port(s):
                    GigabitEthernet1/0/23
        Dynamic host port(s):
                    GigabitEthernet1/0/10
    MAC group(s):
        MAC group address:0100-5e00-0000
        Host port(s): GigabitEthernet1/0/10       GigabitEthernet1/0/23
```

Table 1-1 display igmp-snooping group command output description

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups in all VLANs

Field	Description
Total 1 MAC Group(s).	Total number of MAC multicast groups in all VLANs
Vlan(id):	ID of the VLAN whose multicast group information is displayed
Total 1 IP Group(s).	Total number of IP multicast groups in VLAN 100
Total 1 MAC Group(s).	Total number of MAC multicast groups in VLAN 100
Static Router port(s):	Static router port
Dynamic Router port(s):	Dynamic router port
Static host port(s):	Static member port
Dynamic host port(s):	Dynamic member port
IP group address:	IP address of a multicast group
MAC group(s):	MAC multicast group
MAC group address:	Address of a MAC multicast group
Host port(s)	Member ports

display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Parameters

None

Description

Use the **display igmp-snooping statistics** command to display IGMP Snooping statistics.

This command displays the following information: the numbers of the IGMP general query messages, IGMP group-specific query messages, IGMPv1 report messages, IGMPv2 report messages, IGMP leave messages and error IGMP packets received, and the number of the IGMP group-specific query messages sent.

 **Note**

When IGMPv3 Snooping is enabled, the device makes statistics of IGMPv3 messages as IGMPv2 messages.

Related commands: **igmp-snooping**.

Examples

Display IGMP Snooping statistics.

```
<Sysname> display igmp-snooping statistics
Received IGMP general query packet(s) number:1.
Received IGMP specific query packet(s) number:0.
Received IGMP V1 report packet(s) number:0.
Received IGMP V2 report packet(s) number:3.
Received IGMP leave packet(s) number:0.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:0.
```

The information above shows that IGMP receives:

- one IGMP general query messages
- zero IGMP specific query messages
- zero IGMPv1 report messages
- three IGMPv2 report messages
- zero IGMP leave messages
- zero IGMP error packets

IGMP Snooping sends:

- zero IGMP specific query messages

igmp-snooping

Syntax

igmp-snooping { **enable** | **disable** }

View

System view, VLAN view

Parameters

enable: Enables the IGMP Snooping feature.

disable: Disables the IGMP Snooping feature.

Description

Use the **igmp-snooping enable** command to enable the IGMP Snooping feature.

Use the **igmp-snooping disable** command to disable the IGMP Snooping feature.

By default, the IGMP Snooping feature is disabled.

Caution

- Before enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping setting will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for the IGMP queries. For details, see igmp-snooping vlan-mapping.

Examples

Enable the IGMP Snooping feature on the switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping enable
Enable IGMP-Snooping ok.
```

igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

View

System view, Ethernet port view

Parameters

vlan *vlan-list*: Specifies a VLAN list. With the *vlan-list* argument, you can provide one or more individual VLAN IDs (in the form of *vlan-id*) and/or one or more VLAN ID ranges (in the form of *vlan-id1* **to** *vlan-id2*, where *vlan-id2* must be greater than *vlan-id1*). The effective range for a VLAN ID is 1 to 4094 and the total number of individual VLANs plus VLAN ranges cannot exceed 10.

Description

Use the **igmp-snooping fast-leave** command to enable IGMP fast leave processing.

Use the **undo igmp-snooping fast-leave** command to disable IGMP fast leave processing.

By default, IGMP fast leave processing is disabled.

Note

- The fast leave processing function works for a port only if the host attached to the port runs IGMPv2 or IGMPv3.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).
- If fast leave processing and unknown multicast packet dropping or non-flooding are enabled on a port to which more than one host is connected, when one host leaves a multicast group, the other hosts connected to port and interested in the same multicast group will fail to receive multicast data for that group.

Examples

Enable IGMP fast leave processing on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[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 { **current-interface |** *ip-address* }

undo igmp-snooping general-query source-ip

View

VLAN view

Parameters

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP general queries. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP general queries.

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

Description

Use the **igmp-snooping general-query source-ip** command to configure the source address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the default.

This command can take effect only if the IGMP Snooping querier function is enabled on the switch.

By default, the Layer 2 multicast switch sends general query messages with the source IP address of 0.0.0.0.

Related commands: **igmp-snooping querier**, **igmp-snooping query-interval**.

Examples

Configure the switch to send general query messages with the source IP address 2.2.2.2 in VLAN 3.

```
<Sysname> system-view
System view, return to user view with Ctrl+Z.
[Sysname] igmp-snooping enable
[Sysname] vlan 3
[Sysname-vlan3] igmp-snooping enable
[Sysname-vlan3] igmp-snooping querier
[Sysname-vlan3] igmp-snooping general-query source-ip 2.2.2.2
```

igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*] [**overflow-replace**]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View

Ethernet port view

Parameters

limit: Maximum number of multicast groups the port can join, in the range of 1 to 256.

overflow-replace: Allows a new multicast group to replace an existing multicast group with the lowest IP address.

vlan *vlan-list*: Specifies a VLAN list. With the *vlan-list* argument, you can provide one or more individual VLAN IDs (in the form of *vlan-id*) and/or one or more VLAN ID ranges (in the form of *vlan-id1* **to** *vlan-id2*, where *vlan-id2* must be greater than *vlan-id1*). The effective range for a VLAN ID is 1 to 4094 and the total number of individual VLANs plus VLAN ranges cannot exceed 10.

Description

Use the **igmp-snooping group-limit** command to define the maximum number of multicast groups the port can join.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

If you do not specify any VLAN, the command will take effect for all the VLANs to which the current port belongs; if you specify a VLAN or multiple VLANs, the command will take effect for the port only if the port belongs to the specified VLAN(s). It is recommended to specify a VLAN or multiple VLANs to save memory.

The system default for Switch 4200G series is 256.

Note

- To prevent bursting traffic in the network or performance deterioration of the device caused by excessive multicast groups, you can set the maximum number of multicast groups that the switch should process.
- When the number of multicast groups exceeds the configured limit, the switch removes its multicast forwarding entries starting from the oldest one. In this case, the multicast packets for the removed multicast group(s) will be flooded in the VLAN as unknown multicast packets. As a result, non-member ports can receive multicast packets within a period of time.
- To avoid this from happening, enable the function of dropping unknown multicast packets.
- The keyword overflow-replace does not apply to IGMPv3 Snooping, that is, with IGMPv3 Snooping enabled, even if the keyword overflow-replace is configured, a new multicast group will not replace an existing multicast group when the number of multicast groups reaches the maximum value.
- If an Ethernet port is a static member port for a multicast group, the configuration of the maximum number of multicast groups that can be joined does not take effect on the port.

Examples

Configure to allow GigabitEthernet 1/0/1 in VLAN 2 to join a maximum of 200 multicast groups.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 200 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

System view, Ethernet port view

Parameters

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

vlan *vlan-list*: Specifies a VLAN list. With the *vlan-list* argument, you can provide one or more individual VLAN IDs (in the form of *vlan-id*) and/or one or more VLAN ID ranges (in the form of *vlan-id1* **to** *vlan-id2*, where *vlan-id2* must be greater than *vlan-id1*). The effective range for a VLAN ID is 1 to 4094 and the total number of individual VLANs plus VLAN ranges cannot exceed 10.

Description

Use the **igmp-snooping group-policy** command to configure a multicast group filter.

Use the **undo igmp-snooping group-policy** command to remove the configured multicast group filter.

By default, no multicast group filter is configured.

The ACL rule defines a multicast address or a multicast address range (for example 224.0.0.1 to 239.255.255.255) and is used to:

- Allow the port(s) to join only the multicast group(s) defined in the rule by a permit statement.
- Inhibit the port(s) from joining the multicast group(s) defined in the rule by a deny statement.

Note

- A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.
- If no ACL rule is configured, all the multicast groups will be filtered.
- Since most devices broadcast unknown multicast packets by default, this function is often used together with the function of dropping unknown multicast packets to prevent multicast streams from being broadcast as unknown multicast packets to a port blocked by this function.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Examples

Configure a multicast group filter to allow receivers attached to GigabitEthernet 1/0/1 to access the multicast streams for groups 225.0.0.0 to 225.255.255.255.

- Configure ACL 2000.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[Sysname-acl-basic-2000] quit
```

- Create VLAN 2 and add GigabitEthernet1/0/1 to VLAN 2.

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-vlan2] quit
```

- Apply ACL 2000 on GigabitEthernet1/0/1 to allow it to join only the IGMP multicast groups defined in the rule of ACL 2000.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
[Sysname-GigabitEthernet1/0/1] quit
```

Configure a multicast group filter to allow receivers attached to GigabitEthernet 1/0/2 to access the multicast streams for any groups except groups 225.0.0.0 to 225.0.0.255.

- Configure ACL 2001.

```
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule deny source 225.0.0.0 0.0.0.255
[Sysname-acl-basic-2001] rule permit source any
```

```
[Sysname-acl-basic-2001] quit
```

- Create VLAN 2 and add GigabitEthernet1/0/2 to VLAN 2.

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/2
[Sysname-vlan2] quit
```

- Configure ACL 2001 on GigabitEthernet1/0/2 to it to join any IGMP multicast groups except those defined in the deny rule of ACL 2001.

```
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] igmp-snooping group-policy 2001 vlan 2
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

View

System view

Parameters

seconds: Aging time (in seconds) of multicast member ports, in the range of 200 to 1,000.

Description

Use the **igmp-snooping host-aging-time** command to configure the aging time of multicast member ports.

Use the **undo igmp-snooping host-aging-time** command to restore the default aging time.

By default, the aging time of multicast member ports is 260 seconds.

The aging time of multicast member ports determines the refresh frequency of multicast group members. In an environment where multicast group members change frequently, a relatively shorter aging time is required.

Related commands: **display igmp-snooping configuration**.

Examples

Set the aging time of multicast member ports to 300 seconds.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping host-aging-time 300
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

View

System view

Parameters

seconds: Maximum response time in IGMP general queries, in the range of 1 to 25.

Description

Use the **igmp-snooping max-response-time** command to configure the maximum response time in IGMP general queries.

Use the **undo igmp-snooping max-response-time** command to restore the default.

By default, the maximum response time in IGMP general queries is 10 seconds.

An appropriate setting of the maximum response time in IGMP queries allows hosts to respond to queries quickly and thus the querier can learn the existence of multicast members quickly.

Related commands: **display igmp-snooping configuration**.

Examples

Set the maximum response time in IGMP queries to 15 seconds.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping max-response-time 15
```

igmp-snooping nonflooding-enable

Syntax

igmp-snooping nonflooding-enable

undo igmp-snooping nonflooding-enable

View

System view

Parameters

None

Description

Use the **igmp-snooping nonflooding-enable** command to enable the IGMP Snooping non-flooding function. With this function enabled, unknown multicast packets are passed to the router ports of the switch rather than being flooded in the VLAN.

Use the **undo igmp-snooping nonflooding-enable** command to disable the IGMP Snooping non-flooding function.

By default, the IGMP Snooping non-flooding function is disabled, namely unknown multicast packets are flooded in the VLAN.

The difference between the IGMP Snooping non-flooding function and the function of dropping unknown multicast packets is in that the former passes unknown multicast packets to the router ports while the latter directly discards unknown multicast packets.

You can configure this command only after IGMP Snooping is enabled globally. When IGMP Snooping is disabled globally, the configuration of the **igmp-snooping nonflooding-enable** command is also removed.

Note

If the function of dropping unknown multicast packets is enabled, you cannot enable unknown multicast flooding suppression.

Related commands: **unknown-multicast drop enable**, **multicast-source-deny**, **display multicast-source-deny**

Examples

Enable IGMP Snooping non-flooding after you enable IGMP Snooping globally and disable both port stacking and unknown-multicast dropping.

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

igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

View

VLAN view

Parameters

None

Description

Use the **igmp-snooping querier** command to enable the IGMP Snooping querier feature on the current VLAN.

Use the **undo igmp-snooping querier** command to restore the default.

By default, the IGMP Snooping querier feature is disabled.

This command takes effect only if IGMP Snooping is enabled globally and also enabled in the current VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping query-interval**, **igmp-snooping general-query source-ip**

Examples

Enable the IGMP Snooping querier in VLAN 3.

```
<Sysname> system-view
System view, return to user view with Ctrl+Z.
[Sysname] igmp-snooping enable
```

```
[Sysname] vlan 3
[Sysname-vlan3] igmp-snooping enable
[Sysname-vlan3] igmp-snooping querier
```

igmp-snooping query-interval

Syntax

igmp-snooping query-interval *seconds*

undo igmp-snooping query-interval

View

VLAN view

Parameters

seconds: IGMP query interval, ranging from 1 to 300, in seconds.

Description

Use the **igmp-snooping query-interval** command to configure the IGMP query interval, namely the interval at which the switch sends IGMP general queries.

Use the **undo igmp-snooping query-interval** command to restore the default.

By default, the IGMP query interval is 60 seconds.

These commands are effective only after the IGMP Snooping querier feature is enabled. Otherwise, the switch will not send general queries. The configured query interval must be longer than the maximum response time in general queries.

Related commands: **igmp-snooping enable**, **igmp-snooping querier**, **igmp-snooping max-response-time**, **igmp-snooping general-query source-ip**

Examples

Configure the IGMP query interval to 100 seconds in VLAN 3.

```
<Sysname> system-view
System view, return to user view with Ctrl+Z.
[Sysname] igmp-snooping enable
[Sysname] vlan 3
[Sysname-vlan3] igmp-snooping enable
[Sysname-vlan3] igmp-snooping querier
[Sysname-vlan3] igmp-snooping query-interval 100
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

View

System view

Parameters

seconds: Aging time of router ports, in the range of 1 to 1,000, in seconds.

Description

Use the **igmp-snooping router-aging-time** command to configure the aging time of router ports.

Use the **undo igmp-snooping router-aging-time** command to restore the default aging time.

By default, the aging time of router ports is 105 seconds.

The aging time of router ports should be about 2.5 times the IGMP query interval.

Related commands: **igmp-snooping max-response-time**, **igmp-snooping**.

Examples

Set the aging time of the router port to 500 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping router-aging-time 500
```

igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip { **current-interface** | *ip-address* }

undo igmp-snooping special-query source-ip

View

VLAN view

Parameters

current-interface: Specifies the IP address of the current VLAN interface as the source address to be carried in IGMP group-specific queries. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP group-specific queries.

ip-address: Specifies the source address to be carried in IGMP group-specific queries, which can be any legal IP address.

Description

Use the **igmp-snooping special-query source-ip** command to configure the source address to be carried in IGMP group-specific queries.

Use the undo igmp-snooping special-query source-ip command to restore the default.

By default, the Layer 2 multicast switch sends group-specific query messages with the source IP address of 0.0.0.0.

Related commands: **igmp-snooping querier**.

Examples

Configure the switch to send group-specific query messages with the source IP address 2.2.2.2 in VLAN 3.

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

```
System view, return to user view with Ctrl+Z.
[Sysname] igmp-snooping enable
[Sysname] vlan 3
[Sysname-vlan3] igmp-snooping enable
[Sysname-vlan3] igmp-snooping special-query source-ip 2.2.2.2
```

igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

View

VLAN view

Parameters

version-number: IGMP Snooping version, in the range of 2 to 3 and defaulting to 2.

Description

Use the **igmp-snooping version** command to configure the IGMP Snooping version in the current VLAN.

Use the **undo igmp-snooping version** command to restore the default IGMP Snooping version.

This command can take effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

Set IGMP Snooping version to version 3 in VLAN 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping enable
Enable IGMP-Snooping ok.
[Sysname] vlan 100
[Sysname -vlan100] igmp-snooping enable
[Sysname -vlan100] igmp-snooping version 3
```

igmp-snooping vlan-mapping

Syntax

igmp-snooping vlan-mapping vlan *vlan-id*

undo igmp-snooping vlan-mapping

View

System view

Parameters

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

Description

Use the **igmp-snooping vlan-mapping vlan** command to configure to transmit IGMP general and group-specific query messages in a specific VLAN.

Use the **undo igmp-snooping vlan-mapping** command to restore the default.

By default, the VLAN tag carried in IGMP general and group-specific query messages is not changed.

Examples

Configure IGMP general and group-specific query messages to be transmitted in VLAN 2.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] igmp-snooping enable
[Sysname] igmp-snooping vlan-mapping vlan 2
```

igmp host-join

Syntax

igmp host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

Ethernet port view

Parameters

group-address: Address of the multicast group to join.

source-address: Address of the multicast source to join. You can specify a multicast source address only when IGMPv3 Snooping is running in a VLAN.

vlan *vlan-id*: ID of the VLAN to which the port belongs, in the range of 1 to 4094.

Description

Use the **igmp host-join** command to configure the current port as a simulated multicast group member host to join the specified multicast group or source and group.

Use the **undo igmp host-join** command to remove the current port as a simulated member host for the specified multicast group or source-group.

Unlike a static member port, a port configured as a simulated member host will age out like a dynamic member port.

Related commands: **igmp-snooping enable**, **multicast static-group interface**, **multicast static-group vlan**

Caution

- Before configuring a port as a simulated host, enable IGMP Snooping in VLAN view first.
- The current port must belong to the specified VLAN; otherwise this configuration does not take effect.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 1 as a simulated member host for multicast source 1.1.1.1 and multicast group 225.0.0.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]igmp-snooping enable
  Enable IGMP-Snooping ok.
[Sysname]vlan 1
[Sysname-vlan1]igmp-snooping enable
[Sysname-vlan1]igmp-snooping version 3
[Sysname-vlan1]quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp host-join 225.0.0.1 source-ip 1.1.1.1 vlan 10
```

multicast static-group interface

Syntax

multicast static-group *group-address* **interface** *interface-list*

undo multicast static-group *group-address* **interface** *interface-list*

View

VLAN interface view

Parameters

group-address: IP address of the multicast group to join, in the range of 224.0.0.0 to 239.255.255.255.

interface *interface-list*: Specifies a port list. With the *interface-list* argument, you can define one or more individual ports (in the form of *interface-type interface-number*) and/or one or more port ranges (in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where *interface-number2* must be greater than *interface-number1*). The total number of individual ports plus port ranges cannot exceed 10. For port types and port numbers, refer to the parameter description in the “Port Basic Configuration” part in this manual.

Description

Use the **multicast static-group interface** command to configure the specified port(s) under the current VLAN interface as static member port(s) for the specified multicast group.

Use the **undo multicast static-group interface** command to remove the specified port(s) in the current VLAN as static member port(s) for the specified multicast group.

By default, no port is configured as a static multicast group member port.

Examples

Configure ports GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3 under VLAN-interface 1 as static members ports for multicast group 225.0.0.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] multicast static-group 225.0.0.1 interface GigabitEthernet 1/0/1
to GigabitEthernet 1/0/3
```

multicast static-group vlan

Syntax

multicast static-group *group-address* **vlan** *vlan-id*

undo multicast static-group *group-address* **vlan** *vlan-id*

View

Ethernet port view

Parameters

group-address: IP address of the multicast group to join, in the range of 224.0.0.0 to 239.255.255.255.

vlan *vlan-id*: Specifies the VLAN the Ethernet port belongs to, where *vlan-id* ranges from 1 to 4094.

Description

Use the **multicast static-group vlan** command to configure the current port in the specified VLAN as a static member port for the specified multicast group.

Use the **undo multicast static-group vlan** command to remove the current port in the specified VLAN as a static member port for the specified multicast group.

By default, no port is configured as a static multicast group member port.

Examples

Configure port GigabitEthernet1/0/1 in VLAN 2 as a static member port for multicast group 225.0.0.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast static-group 225.0.0.1 vlan 2
```

multicast static-router-port

Syntax

multicast static-router-port *interface-type interface-number*

undo multicast static-router-port *interface-type interface-number*

View

VLAN view

Parameters

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

Description

Use the **multicast static-router-port** command to configure the specified port in the current VLAN as a static router port.

Use the **undo multicast static-router-port** command to remove the specified port in the current VLAN as a static router port.

By default, a port is not a static router port.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 10 as a static router port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 10
[Sysname-vlan10] multicast static-router-port GigabitEthernet1/0/1
```

multicast static-router-port vlan

Syntax

multicast static-router-port vlan *vlan-id*

undo multicast static-router-port vlan *vlan-id*

View

Ethernet port view

Parameters

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

Description

Use the **multicast static-router-port vlan** command to configure the current port in the specified VLAN as a static router port.

Use the **undo multicast static-router-port vlan** command to remove the current port in the specified VLAN as a static router port.

By default, the static router port function is disabled.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 10 as a static router port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast static-router-port vlan 10
```

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Parameters

None

Description

Use the **reset igmp-snooping statistics** command to clear IGMP Snooping statistics.

Related commands: **display igmp-snooping statistics**.

Examples

Clear IGMP Snooping statistics.

```
<Sysname> reset igmp-snooping statistics
```

service-type multicast

Syntax

service-type multicast

undo service-type multicast

View

VLAN view

Parameters

None

Description

Use the **service-type multicast** command to configure the current VLAN as a multicast VLAN.

Use the **undo service-type multicast** command to remove the current VLAN as a multicast VLAN.

By default, no VLAN is a multicast VLAN.

In an IGMP Snooping environment, by configuring a multicast VLAN and adding ports to the multicast VLAN, you can allow users in different VLANs to share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN. In addition, because the multicast VLAN is isolated from user VLANs, this method also enhances the information security.

Note

- One port belongs to only one multicast VLAN.
- The port connected to a user terminal must be a hybrid port.
- The multicast member port must be in the same multicast VLAN with the router port. Otherwise, the port cannot receive multicast packets.
- If a router port is in a multicast VLAN, the router port must be configured as a trunk port or a hybrid port that allows tagged packets to pass for the multicast VLAN. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.
- If a multicast member port needs to receive multicast packets forwarded by a router port that does not belong to any multicast VLAN, the multicast member port must be removed from the multicast VLAN. Otherwise, the port cannot receive multicast packets.

Examples

Configure VLAN 2 as a multicast VLAN.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan 2
[Sysname-vlan2] service-type multicast
```

2 Common Multicast Configuration Commands

Common Multicast Configuration Commands

display mac-address multicast

Syntax

display mac-address multicast [**static** [{ { *mac-address* **vlan** *vlan-id* | **vlan** *vlan-id* } [**count**] } | **count**]]

View

Any view

Parameter

static: Displays static multicast MAC address entries.

mac-address **vlan** *vlan-id*: Displays multicast MAC address entry/entries in the specified VLAN.

count: Displays the number of MAC entries.

vlan *vlan-id*: ID of the specific VLAN.

Description

Use the **display mac-address multicast** command to display the multicast MAC address entry/entries manually configured on the switch.

- Executing this command with neither *mac-address* **vlan** *vlan-id* nor **vlan** *vlan-id* will display the information about all the multicast MAC address entries manually added on the switch, including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.
- Executing this command with **vlan** *vlan-id* but without mac-address will display the information about all the multicast MAC address entries manually added in the specified VLAN, including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.
- Executing this command with both **mac-address** and **vlan** *vlan-id* will display the information about the multicast MAC address entries manually added in the specified VLAN with the specified multicast MAC address, including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.
- Executing this command with **count** will display the information about the number of multicast MAC address entries added on the switch.

Example

Display all the multicast MAC address entries manually added in VLAN 1.

```
<Sysname> display mac-address multicast static vlan 1
MAC ADDR          VLAN ID STATE           PORT INDEX             AGING TIME(s)
0100-0001-0001    1       Config static   GigabitEthernet1/0/1   N/A
                                          GigabitEthernet1/0/2
                                          GigabitEthernet1/0/3
```

```
                                        GigabitEthernet1/0/4
---  1 static mac address(es) found  ---
```

Table 2-1 display mac-address multicast static command output description

Field	Description
MAC ADDR	MAC address
VLAN ID	The VLAN in which the MAC address is manually added
STATE	State of the MAC address, which includes only **Config static**, indicating that the table entry is manually added.
PORT INDEX	Ports out which the multicast packets destined for the multicast MAC address are forwarded
AGING TIME(s)	Remaining lifetime of the entry. **N/A** indicates that the entry never expires.

mac-address multicast interface

Syntax

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address multicast [*mac-address* [**interface** *interface-list*] **vlan** *vlan-id*]

View

System view

Parameters

mac-address: Multicast MAC address, in the form of H-H-H.

interface *interface-list*: Specifies forwarding ports for the specified multicast MAC group address. With the *interface-list* argument, you can define one or more individual ports (in the form of *interface-type interface-number*) and/or one or more port ranges (in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where *interface-number2* must be greater than *interface-number1*). The total number of individual ports plus port ranges cannot exceed 10. For port types and port numbers, refer to the parameter description in the “Port Basic Configuration” part in this manual.

vlan *vlan-id*: Specifies the VLAN to which the forwarding ports belong. The effective range for *vlan-id* is 1 to 4094.

Description

Use the **mac-address multicast interface** command to create a multicast MAC address entry.

Use the **undo mac-address multicast interface** command to remove the specified multicast MAC address entry or all multicast MAC address entries.

Each multicast MAC address entry contains multicast address, forward port, VLAN ID, and so on.

Related commands: **display mac-address multicast static**.

Examples

Create a multicast MAC address entry, with the multicast MAC address of 0100-5c0a-0805 and a forwarding port of GigabitEthernet 1/0/1 in VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] mac-address multicast 0100-5c0a-0805 interface GigabitEthernet 1/0/1 vlan 1
```

mac-address multicast vlan

Syntax

mac-address multicast *mac-address* **vlan** *vlan-id*

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

View

Ethernet port view

Parameters

mac-address: Multicast MAC address in the form of H-H-H.

vlan *vlan-id*: Specifies the VLAN the current port belongs to. The effective range for *vlan-id* is 1 to 4094.

Description

Use the **mac-address multicast vlan** command to create a multicast MAC address entry on the current port.

Use the **undo mac-address multicast vlan** command to remove the specified multicast MAC address entry or all multicast MAC address entries on the current port.

Each multicast MAC address entry contains the multicast address, forwarding port, and VLAN ID information.

Related commands: **display mac-address multicast static**.

Examples

Create a multicast MAC address entry on GigabitEthernet 1/0/1 in VLAN 1, with the multicast address of 0100-1000-1000.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-1000-1000 vlan 1
```

unknown-multicast drop enable

Syntax

unknown-multicast drop enable

undo unknown-multicast drop enable

View

System view

Parameters

None

Description

Use the **unknown-multicast drop enable** command to enable the function of dropping unknown multicast packets.

Use the **undo unknown-multicast drop enable** command to disable the function of dropping unknown multicast packets.

By default, the function of dropping unknown multicast packets is disabled.

Examples

Enable the unknown multicast drop feature.

```
<Sysname> system-view
System view: return to user view with Ctrl+Z.
[Sysname] unknown-multicast drop enable
```

Table of Contents

1 NTP Configuration Commands

Note

To protect unused sockets against attacks by malicious users and improve security, 3Com S4200G series Ethernet switches provide the following functions:

- UDP port 123 is opened only when the NTP feature is enabled.
- UDP port 123 is closed as the NTP feature is disabled.

These functions are implemented as follows:

- Execution of one of the **ntp-service unicast-server**, **ntp-service unicast-peer**, **ntp-service broadcast-client**, **ntp-service broadcast-server**, **ntp-service multicast-client**, and **ntp-service multicast-server** commands enables the NTP feature and opens UDP port 123 at the same time.
- Execution of the **undo** form of one of the above six commands disables all implementation modes of the NTP feature and closes UDP port 123 at the same time.

NTP Configuration Commands

display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

Any view

Parameters

verbose: Displays the detailed information about all the sessions maintained by the NTP service. Without this keyword, the command displays the brief information about all the sessions.

Description

Use the **display ntp-service sessions** command to display the information about all the sessions maintained by local NTP services.

Examples

View the brief information of all sessions maintained by NTP services.

```
<Sysname> display ntp-service sessions
     source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]3.0.1.32    LOCL                1    95   64   42  -14.3   12.9    2.7
```

```
[25]3.0.1.31    127.127.1.0          2     1    64    1 4408.6   38.7    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  2
```

Table 1-1 Description on the fields of the **display ntp-service sessions** command

Field	Description
source	IP address of the synchronization source
reference	Reference clock ID of the synchronization source 1) If the reference clock is the local clock, the value of this field is related to the value of the **stra** field: • When the value of the **stra** field is 0 or 1, this field will be “LOCL”; • When the **stra** field has another value, this filed will be the IP address of the local clock. 2) If the reference clock is the clock of another switch on the network, the value of this field will be the IP address of that switch.
stra	Stratum of the clock of the synchronization source
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable
poll	Polling interval in seconds, that is, the maximum interval between two successive messages
now	Time elapsing since the last NTP packet is sent
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	Network delay, that is, the roundtrip delay from the local switch to the clock source, in milliseconds
disper	Maximum offset of the local clock relative to the reference clock
[12345]	1: Clock source selected by the system, namely the current reference source, with a system clock stratum level smaller than or equal to 15 2: Stratum level of this clock source is smaller than or equal to 15 3: This clock source has passed the clock selection process 4: This clock source is a candidate clock source 5: This clock source was created by a configuration command
Total associations	Total number of associations

Caution

An S4200G series switch does not establish a session with its client when it works in the NTP server mode, but does so when it works in other NTP implementation modes.

display ntp-service status

Syntax

display ntp-service status

View

Any view

Parameters

None

Description

Use the **display ntp-service status** command to display the status of NTP services.

Examples

View the status of the NTP service of the local switch.

```
<Sysname> display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 1.1.1.11
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.8174 ms
 Root delay: 37.86 ms
 Root dispersion: 45.98 ms
 Peer dispersion: 35.78 ms
 Reference time: 16:30:46.078 UTC Mar 29 2007(C9689FB6.1431593E)
```

Table 1-2 Description on the fields of the **display ntp-service status** command

Field	Description
Clock status	Status of the local clock: • Synchronized • Unsynchronized
Clock stratum	Stratum of the local clock
Reference clock ID	Address of the remote server or ID of the reference clock after the local clock is synchronized to a remote NTP server or a reference clock
Nominal frequency	Nominal frequency of the local hardware clock, in Hz.
Actual frequency	Actual frequency of the local hardware clock, in Hz.
Clock precision	Precision of the local hardware clock
Clock offset	Offset of the local clock relative to the reference clock, in milliseconds.
Root delay	Roundtrip delay between the local clock and the primary reference clock source, in milliseconds.
Root dispersion	Maximum dispersion of the local clock relative to the primary reference clock, in milliseconds.
Peer dispersion	Maximum dispersion of the remote NTP server, in milliseconds.
Reference time	Reference timestamp

display ntp-service trace

Syntax

display ntp-service trace

View

Any view

Parameters

None

Description

Use the **display ntp-service trace** command to display the brief information of each NTP time server along the time synchronization chain from the local switch to the reference clock source.

Examples

View the brief information of each NTP time server along the time synchronization chain from the local switch to the reference clock source.

```
<Sysname> display ntp-service trace
server4: stratum 4, offset 0.0019529, synch distance 0.144135
server3: stratum 3, offset 0.0124263, synch distance 0.115784
server2: stratum 2, offset 0.0019298, synch distance 0.011993
server1: stratum 1, offset 0.0019298, synch distance 0.011993 refid  'GPS Receiver'
```

The above information displays the time synchronization chain of server4: server4 is synchronized to server3, server3 to server2, server2 to server1, and server1 to the reference clock source GPS receiver.

ntp-service access

Syntax

ntp-service access { **peer** | **server** | **synchronization** | **query** } *acl-number*

undo ntp-service access { **peer** | **server** | **synchronization** | **query** }

View

System view

Parameters

query: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called “control query” refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.

synchronization: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.

server: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.

peer: Peer right. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the peer device.

acl-number: Basic Access Control List (ACL) number, in the range of 2000 to 2999.

Description

Use the **ntp-service access** command to set the access control right from the remote device to the local NTP server.

Use the **undo ntp-service access** command to remove the configured access control right to the local NTP server.

By default, the access control right from the remote device to the local NTP server is **peer**.

NTP service access-control rights from the highest to the lowest are **peer**, **server**, **synchronization**, and **query**. When a local NTP server receives an NTP request, it will perform an access-control right match and will use the first matched right.

The **ntp-service access** command only provides a minimal degree of security measure. A more secure way is to perform identity authentication.

Refer to the **ntp-service authentication enable** command for related configuration.

Examples

Configure the access right from the remote device in ACL 2076 to the local NTP server as **peer**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service access peer 2076
```

Configure the access right from the remote device in ACL 2028 to the local NTP server as **server**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service access server 2028
```

ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

View

System view

Parameters

None

Description

Use the **ntp-service authentication enable** command to enable the NTP authentication.

Use the **undo ntp-service authentication enable** command to disable the NTP authentication.

By default, the NTP authentication is disabled.

Refer to the **ntp-service reliable authentication-keyid** and **ntp-service authentication-keyid** commands for related configuration.

Examples

Enable the NTP authentication.

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

ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *key-id* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *key-id*

View

System view

Parameters

key-id: Authentication key ID, in the range of 1 to 4294967295.

value: Authentication key, a string comprising 1 to 32 characters. Up to 1024 keys can be configured.

Description

Use the **ntp-service authentication-keyid** command to configure an NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove an NTP authentication key.

By default, no NTP authentication key is configured.

Currently, the system only supports the Message Digest 5 (MD5) algorithm.

After configuring the NTP authentication key, you need to use the **ntp-service reliable authentication-keyid** command to specify the authentication key as a trusted key.

Related commands: **ntp-service reliable authentication-keyid**.

Examples

Configure an MD5 authentication key, with the key ID being 10 and the key being BetterKey.

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

Parameters

None

Description

Use the **ntp-service broadcast-client** command to configure an Ethernet switch to operate in the NTP broadcast client mode and receive NTP broadcast messages through the current interface.

Use the **undo ntp-service broadcast-client** command to remove the configuration.

By default, no NTP operate mode is configured.

Examples

Configure the switch to operate in the broadcast client mode and receive NTP broadcast messages through VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *key-id* | **version** *number*]*

undo ntp-service broadcast-server

View

VLAN interface view

Parameters

authentication-keyid *key-id*: Specifies the key ID used for sending messages to broadcast clients. The *key-id* argument ranges from 1 to 4294967295. You do not need to configure **authentication-keyid** *key-id* if authentication is not required.

version *number*: Specifies the NTP version number which ranges from 1 to 3. The default version number is 3.

Description

Use the **ntp-service broadcast-server** command to configure an Ethernet switch to operate in the NTP broadcast server mode and send NTP broadcast messages through the current interface.

Use the **undo ntp-service broadcast-server** command to remove the configuration.

By default, no NTP operate mode is configured.

Examples

Configure the switch to send NTP broadcast messages through VLAN-interface 1 and use authentication key 4 for encryption, and set the NTP version number to 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
```

```
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-key 4 version 3
```

ntp-service in-interface disable

Syntax

ntp-service in-interface disable

undo ntp-service in-interface disable

View

VLAN interface view

Parameters

None

Description

Use the **ntp-service in-interface disable** command to disable the interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, the interface can receive NTP messages.

Examples

Disable VLAN-interface 1 from receiving NTP messages.

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

Parameters

number: Maximum number of the dynamic NTP sessions that can be established locally. This argument ranges from 0 to 100.

Description

Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions that can be established locally.

Use the **undo ntp-service max-dynamic-sessions** command to restore the default.

By default, up to 100 dynamic NTP sessions can be established locally.

Examples

Set the maximum number of dynamic NTP sessions that can be established locally to 50.

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

Parameters

ip-address: Multicast IP address, in the range of 224.0.1.0 to 224.0.1.255. The default IP address is 224.0.1.1.

Description

Use the **ntp-service multicast-client** command to configure an Ethernet switch to operate in the NTP multicast client mode and receive NTP multicast messages through the current interface.

Use the **undo ntp-service multicast-client** command to remove the configuration.

By default, no NTP operate mode is configured.

Examples

Configure the switch to receive NTP multicast messages through VLAN-interface 1, with the multicast IP address being 224.0.1.2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.2
```

ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **version** *number*]*

undo ntp-service multicast-server [*ip-address*]

View

VLAN interface view

Parameters

ip-address: Multicast IP address, in the range of 224.0.1.0 to 224.0.1.255. The default IP address is 224.0.1.1.

authentication-keyid *key-id*: Specifies the key ID used for sending messages to multicast clients. The *key-id* argument ranges from 1 to 4294967295.

ttl *ttl-number*: Defines the lifetime of multicast messages. The *ttl-number* argument ranges from 1 to 255 and defaults to 16.

version *number*: Specifies the NTP version number which ranges from 1 to 3 and defaults to 3.

Description

Use the **ntp-service multicast-server** command to configure an Ethernet switch to operate in the NTP multicast server mode and send NTP multicast messages through the current interface.

Use the **undo ntp-service multicast-server** command to remove the configuration.

By default, no NTP operate mode is configured.

Examples

Configure the switch to send NTP multicast messages through VLAN-interface 1, and set the multicast group address to 224.0.1.2, keyid to 4, and the NTP version number to 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1]ntp-service multicast-server 224.0.1.2
authentication-keyid 4 version 2
```

ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *key-id*

undo ntp-service reliable authentication-keyid *key-id*

View

System view

Parameters

key-id: Authentication key ID, in the range of 1 to 4294967295.

Description

Use the **ntp-service reliable authentication-keyid** command to specify an authentication key as a trusted key.

Use the **undo ntp-service reliable authentication-keyid** command to remove the configuration.

By default, no trusted key is configured.

When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Related commands: **ntp-service authentication-keyid**.

Examples

Enable NTP authentication. The encryption algorithm is MD5, the key ID is 37, and the trusted key is **abc**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 abc
```

Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax

ntp-service source-interface Vlan-interface *vlan-id*

undo ntp-service source-interface

View

System view

Parameters

vlan-interface *vlan-id*: Specifies an interface. The IP address of the interface serves as the source IP address of sent NTP messages. The *vlan-id* argument indicates the ID of the specified VLAN interface, ranging from 1 to 4094.

Description

Use the **ntp-service source-interface** command to specify a VLAN interface through which NTP messages are to be sent.

Use the **undo ntp-service source-interface** command to remove the configuration.

If you do not want the IP addresses of the other interfaces on the local switch to be the destination addresses of response messages, you can use this command to specify a specific interface to send all NTP packets. In this way, the IP address of the interface is the source IP address of all NTP messages sent by the local device.

Examples

Specify the source IP addresses of all sent NTP messages as the IP address of VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service source-interface Vlan-interface 1
```

ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *remote-ip* | *peer-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*

undo ntp-service unicast-peer { *remote-ip* | *peer-name* }

View

System view

Parameters

remote-ip: IP address of the NTP symmetric-passive peer. This argument can be a unicast address only, and cannot be a broadcast address, a multicast address, or the IP address of the local reference clock.

peer-name: Symmetric-passive peer host name, a string comprising 1 to 20 characters.

authentication-keyid *key-id*: Specifies the key ID used for sending messages to the peer. The *key-id* argument ranges from 1 to 4294967295. By default, authentication is not enabled.

priority: Specifies the peer identified by the *remote-ip* argument as the preferred peer for synchronization.

source-interface Vlan-interface *vlan-id*: Specifies an interface whose IP address serves as the source IP address of NTP message sent to the peer. *vlan-id* is the VLAN interface number.

version *number*: Specifies the NTP version number. The version number ranges from 1 to 3 and defaults to 3.

Description

Use the **ntp-service unicast-peer** command to configure an Ethernet switch to operate in the symmetric-active peer mode.

Use the **undo ntp-service unicast-peer** command to remove the configuration.

By default, no NTP operate mode is configured.

Note

If you use *remote-ip* or *peer-name* to specify a remote device as the peer of the local Ethernet switch, the local switch operates in the symmetric-active peer mode. In this case, the clock of local Ethernet switch and that of the remote device can be synchronized to each other.

Examples

Configure the local switch to obtain time information from the peer with the IP address 128.108.22.44 and also to provide time information to the peer. Set the NTP version number to 3. The source IP address of NTP messages is the IP address of Vlan- interface1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service unicast-peer 128.108.22.44 version 3 source-interface Vlan-interface
1
```

ntp-service unicast-server

Syntax

ntp-service unicast-server { *remote-ip* | *server-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*

undo ntp-service unicast-server { *remote-ip* | *server-name* }

View

System view

Parameters

remote-ip: IP address of an NTP server. This argument can be a unicast address only, and cannot be a broadcast address, multicast group address, or IP address of the local clock.

server-name: NTP server name, a string comprising 1 to 20 characters.

authentication-keyid *key-id*: Specifies the key ID used for sending messages to the NTP server. The *key-id* argument ranges from 1 to 4294967295.

priority: Specifies the server identified by the *remote-ip* or the *server-name* argument as the preferred server.

source-interface Vlan-interface *vlan-id*: Specifies an interface whose IP address serves as the source IP address of NTP packets sent by the local switch to the server.

version *number*: Specifies the NTP version number. The *number* argument ranges from 1 to 3 and defaults to 3.

Description

Use the **ntp-service unicast-server** command to configure an Ethernet switch to operate in the NTP client mode.

Use the **undo ntp-service unicast-server** command to remove the configuration.

By default, no NTP operate mode is configured.

Note

The remote server specified by *remote-ip* or *server-name* serves as the NTP server, and the local switch serves as the NTP client. The clock of the NTP client will be synchronized by but will not synchronize that of the NTP server.

Examples

Configure the local switch to be synchronized to the NTP server with the IP address 128.108.22.44, and set the version number to 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ntp-service unicast-server 128.108.22.44 version 3
```

Table of Contents

1 SSH Commands

Note

In this document, you can distinguish the local and peer as follows: if the local is an SSH server, the peer is an SSH client; if the local is an SSH client, the peer is an SSH server.

SSH Commands

display public-key local

Syntax

display public-key local { **dsa | rsa** } **public**

View

Any view

Parameters

dsa: Displays the public key of the current switch's DSA key pair.

rsa: Displays the public keys of the current switch's RSA key pairs.

Description

Use the **display public-key local** command to display the public key information of the current switch's key pairs.

The displayed local public key can be configured as the public key on the remote peer for authentication.

Related commands: **public-key local create**.

Examples

Display the public key part of the current switch's RSA key pair(s).

```
<Sysname> display public-key local rsa public

=====================================================
Time of Key pair created: 23:48:18  2000/04/03
Key name: Sysname_Host
Key type: RSA encryption Key
=====================================================
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100C7C4D2E1C59A75908417C660AD1D5E
B172AB6EE9AAF994DB7A1C31EB87F750EE12A57832C6070FC008A5EE2B6675FD6A430575D97350E300A20FEB
773D93D7C3565467B0CA6B95C07D3338C523743B49D82C5EC2C9458D248955846F9C32F4D25CC92D0E831E56
4BBA6FAE794EEC6FCDEDB822909CC687BEBF51F3DFC5C30D590203010001

=========================================================
Time of Key pair created: 23:48:36  2000/04/03
Key name: Sysname_Server
Key type: RSA encryption Key
=========================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100BC86D8F08E101461C1231B122777DBE777645C
81C569C004EC2FEC03C205CC7E3B5DAA38DD865C6D1FB61C91B85ED63C6F35BAFBF9A6D2D2989C20051FF8FA
31A14FCF73EC1485422E5B800B55920FC121329020E82F2945FFAD81BE72663BF70203010001
```

Display the public key of the current switch's DSA key pair.

```
<Sysname> display public-key local dsa public

=========================================================
Time of Key pair created: 08:01:23  2000/04/02
Key name:
Key type: DSA encryption Key
=========================================================
Key code:
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F0A4
23F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26CCB987
723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F0678D7722B53
41C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F
0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B
20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B612391C76C1FB2
E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF
038184000281804B7E6A5D60A6B71C0B585ED495C36F82C17072C0446CE099F2C733171E8C014B6D4F91C54C
9998921CA35C7BD4385E55D39B324F04DBE9F4CC91DE8ED949C7007C160D129ECB54D6C39E697DAD5BFB56BA
F3281584B23CA7DFB46AAB5B8C56A5903F61B34A157022E68C6C2423D42B880FB20BA86135369F7CF3ACA46A
55BEF8
```

display public-key peer

Syntax

display public-key peer [**brief** | **name** *pubkey-name*]

View

Any view

Parameters

brief: Displays brief information about the locally saved public keys of all SSH peers.

pubkey-name: Name of the public key, a string of 1 to 64 characters.

Description

Use the **display public-key peer** command to display information about locally saved public keys of the SSH peers. If no key name is specified, the command displays detailed information about the locally saved public keys of all SSH peers.

The **display public-key peer** command on the SSH server displays the locally saved public keys of SSH clients while the command on the SSH client displays the locally saved keys of the SSH servers.

Caution

Sometimes the public key modulus displayed with the **display public-key peer** command is one bit smaller than the actual modulus. This is because the actually generated key pair is one bit smaller than specified. For example, when you specify a 1024-bit key pair, the actually generated key pair may have 1024 or 1023 bits.

Note

You can configure an SSH peer's public key on the current switch by using the **public-key peer** command or the **public-key peer import sshkey** command.

Related commands: **public-key peer**, **public-key peer import sshkey**.

Examples

Display brief information about all peer public keys.

```
<Sysname> display public-key peer brief
Type  Module  Name
--------------------------
RSA   1023    idrsa
DSA   1024    127.0.0.1
RSA   1024    18
```

Display the information about the public key named pubkey-name.

```
<Sysname> display public-key peer name pubkey-name
=====================================
  Key name  : pubkey-name
  Key type  : RSA
  Key module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B003081870281810 09C46A8710216CEC0C01C7CE136BA76
C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB7442D563
93BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A775
7C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

display rsa local-key-pair public

Syntax

display rsa local-key-pair public

View

Any view

Parameters

None

Description

Use the **display rsa local-key-pair public** command to display the public keys of the current switch's RSA key pairs. If no key pair has been generated, the system displays a message, telling you that no RSA keys are found..

Related commands: **rsa local-key-pair create**.

Examples

Display the public keys of the current switch's RSA key pairs.

```
<Sysname> display rsa local-key-pair public

=====================================================
Time of Key pair created: 20:08:35  2000/04/02
Key name: Sysname_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    DE99B540 87B666B9 69C948CD BBCC2B60 997F9C18
    9AA6651C 6066EF76 242DEAD1 DEFEA162 61677BD4
    1A7BFAE7 668EDAA9 FB048C37 A0F1354D 5798C202
    2253F4F5
  0203
    010001

=====================================================
Time of Key pair created: 20:08:46  2000/04/02
Key name: Sysname_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    D6D70AE4 D2A900BE AC21B4E7 617CBEFA 2BAED61F
    B637070C 093F43AF 9DB9D644 BCD921EF D056EF36
    26825C2A 1FC0EFC3 E27B5110 3F20F790 6C83274B
```

```
    D0FC303F 51072D6C B5D0054D 3673EBA0 A4748984
    5EBF6EBE CF6A13B1 C7858241 A2A9AA79
  0203
    010001
```

Note

After you complete the RSA key pair generation task:

- If the switch is working in SSH1-compatible mode, there should be two public keys generated (that is, the host public key and the server public key), and the **display rsa local-key-pair public** command should display those two public keys.
- If the switch is working in SSH2 mode, there should be only one public key generated (that is, the host public key), and the command should display the public key.

---

display rsa peer-public-key

Syntax

display rsa peer-public-key [**brief** | **name** *keyname*]

View

Any view

Parameters

brief: Displays brief information about the public keys of all SSH peers.

keyname: Specifies a key by its name, which is a string of 1 to 64 characters.

Description

Use the **display rsa peer-public-key** command to display information about the locally saved public keys of all SSH peers. If no key name is specified, the command displays detailed information about the locally saved public keys of all SSH peers.

The **display rsa peer-public-key** command on the SSH server displays the locally saved public keys of the SSH clients while the command on the SSH client displays the locally saved key of the SSH servers.

Caution

Sometimes the public key modulus displayed with the display rsa peer-public-key command is one bit smaller than the actual modulus. This is because the actually generated key pair is one bit smaller than specified. For example, when you specify a 1024-bit key pair, the actually generated key pair may have 1024 or 1023 bits.

Examples

Display brief information about all peer public keys.

```
<Sysname> display rsa peer-public-key brief
Type  Module  Name
---------------------------
DSA   1023    2
DSA   1024    a
```

Display the information about public key “abcd”.

```
<Sysname> display rsa peer-public-key name abcd


=====================================
  Key name  : abcd
  Key type  : RSA
  Key module: 1024
=====================================
Key Code:
30819F300D06092A864886F70D010101050003818D0030818902818100B0EEC8768E310AE2EE44D65A2F944E
2E6F32290D1ECBBFFF22AA11712151FC29F1C1CD6D7937723F77103576C41A03DB32F32C46DEDA68566E89B5
3CD4DF8F9899B138C578F7666BFB5E6FE1278A84EC8562A12ACBE2A43AF61394276CE5AAF5AF01DA8B0F33E0
8335E0C3820911B90BF4D19085CADCE0B50611B9F6696D31930203010001
```

display ssh server

Syntax

display ssh server { **session** | **status** }

View

Any view

Parameters

session: Displays SSH session information.

status: Displays SSH status information.

Description

Use the **display ssh server** command on an SSH server to display information about SSH status or about sessions of active connections with SSH clients.

Related commands: **ssh server authentication-retries**, **ssh server timeout**, **ssh server compatible-ssh1x enable**, **ssh server rekey-interval**.

Examples

Display status information about the SSH Server.

```
<Sysname> display ssh server status
 SSH version : 1.99
 SSH connection timeout : 60 seconds
 SSH server key generating interval : 0 hours
```

```
SSH Authentication retries : 3 times
SFTP Server: Disable
SFTP idle timeout : 10 minutes
```

Caution

- If you use the **ssh server compatible-ssh1x enable** command to configure the server to be compatible with SSH1.x clients, the SSH version will be displayed as 1.99.
- If you use the **undo ssh server compatible-ssh1x** command to configure the server to be not compatible with SSH1.x clients, the SSH version will be displayed as 2.0.

Display information about sessions of active connection with SSH clients.

```
<Sysname> display ssh server session
 Conn    Ver   Encry    State     Retry    SerType  Username
 VTY 0   2.0   AES      started   0        stelnet  kk
 VTY 1   2.0   AES      started   0        sFTP     abc
```

Table 1-1 Description on the fields of the **display ssh server session** command

Field	Description
Conn	Number of VTY interface used for user login
Ver	SSH version
Encry	Encryption algorithm used by SSH
State	Session status
Retry	Number of connection retries
SerType	Service type
Username	User name

display ssh server-info

Syntax

display ssh server-info

View

Any view

Parameters

None

Description

Use the **display ssh server-info** command on an SSH client to display the mappings between SSH servers and their public keys saved on the client.

Note

If an SSH client needs to authenticate the SSH server, it uses the locally saved public key of the server for authentication. In case the authentication fails, you can use the **display ssh server-info** command to view whether the locally saved public key of the server is correct.

Related commands: **ssh client assign**, **ssh client first-time enable**.

Examples

Display the mappings between SSH servers and their public keys saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP)                                 Server public key name
_____________________________________________________________________

192.168.0.90                                    192.168.0.90
```

display ssh user-information

Syntax

display ssh user-information [*username*]

View

Any view

Parameters

username: SSH user name, a string of 1 to 184 characters. It cannot contain any of these characters: slash (/), backslash (\), colon (:), asterisk (*), question mark (?), less than sign (<), greater than sign (>), and the vertical bar sign (|). In addition, the @ sign can appear up to once, the username part (that is, the string before the @ sign) cannot be more than 55 characters, and the domain name part cannot be more than 128 characters.

Description

Use the **display ssh user-information** command on an SSH server to display information about all SSH users, including user name, authentication type, corresponding public key name and authorized service type. If the *username* argument is specified, the command displays information about the specified user.

Related commands: **ssh authentication-type default**, **ssh user**, **ssh user authentication-type, ssh user assign**, **ssh user service-type**.

Examples

Create an SSH user named **client** and specify publickey authentication as the authentication mode for the SSH user.

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

```
[Sysname] ssh user client authentication-type publickey
```

Configure SFTP as the service type for the SSH user.

```
[Sysname] ssh user client service-type sftp
```

Assign the public key **test** for the SSH user.

```
[Sysname] ssh user client assign publickey test
```

Display information about the SSH user configured on the SSH server.

```
[Sysname] display ssh user-information
 Username            Authentication-type  User-public-key-name  Service-type
 client                 publickey            test                  sftp
```

display ssh2 source-ip

Syntax

display ssh2 source-ip

View

Any view

Parameters

None

Description

Use the **display ssh2 source-ip** command to display the current source IP address or the IP address of the source interface specified for the SSH client. If neither source IP address nor source interface is specified, the command displays 0.0.0.0.

Related commands: **ssh2 source-ip**.

Examples

Display the current source IP address specified for the SSH Client.

```
<Sysname> display ssh2 source-ip
The source IP you specified is 192.168.0.1
```

display ssh-server source-ip

Syntax

display ssh-server source-ip

View

Any view

Parameters

None

Description

Use the **display ssh-server source-ip** command to display the current source IP address or the IP address of the source interface specified for the SSH server. If neither source IP address nor source interface is specified, the command displays 0.0.0.0.

Related commands: **ssh-server source-ip**.

Examples

Display the current source IP address specified for the SSH Server.

```
<Sysname> display ssh-server source-ip
The source IP you specified is 192.168.1.1
```

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Parameters

None

Description

Use the **peer-public-key end** command to return from public key view to system view.

Related commands: **rsa peer-public-key**, **public-key-code begin**, **public-key peer**.

Examples

Exit public key view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa peer-public-key Switch003
RSA public key view: return to System View with "peer-public-key end".
[Sysname-rsa-public-key] peer-public-key end
[Sysname]
```

protocol inbound

Syntax

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

View

VTY user interface view

Parameters

all: Supports both Telnet and SSH.

ssh: Supports only SSH.

Description

Use the **protocol inbound** command to configure specific user interface(s) to support specified protocol(s). The configuration will take effect at next user login.

By default, both SSH and Telnet are supported.

Note

As SSH clients access the SSH server through VTY user interfaces, you need configure the VTY user interfaces of the SSH server to support remote SSH login.

Caution

- If you have configured a user interface to support SSH protocol, to ensure a successful login to the user interface, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command.
- For a user interface, if you have executed the **authentication-mode password** or **authentication-mode none** command, the **protocol inbound ssh** command cannot be executed; if you have executed the **protocol inbound ssh** command, neither of the **authentication-mode password** and **authentication-mode none** commands can be executed.

Examples

Configure vty0 through vty4 to support SSH only.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

public-key local create

Syntax

public-key local create { **dsa** | **rsa** }

View

System view

Parameters

dsa: Specifies the DSA key pair.

rsa: Specifies the RSA key pair.

Description

Use the **public-key local create** command to create a local DSA key pair or RSA key pairs.

Note that:

- Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.
- After entering this command, you will be prompted to provide the length of the key modulus. The length is in the range 512 to 2048 bits and defaults to 1024 bits. If the key pair already exists, the system will ask you whether you want to overwrite it.
- The key pair created by this command can survive a reboot. You only need to configure it once.

Related commands: **public-key local destroy**, **display public-key local**.

Examples

Create local RSA key pairs.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[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.
Input the bits in the modulus[default = 1024]:
Generating keys...
...++++++
.....++++++
.....++++++++
.....++++++++
......
```

Display the public key information of the local RSA key pairs.

```
[Sysname] display public-key local rsa public

=====================================================
Time of Key pair created: 03:14:23  2000/04/06
Key name: Sysname_Host
Key type: RSA encryption Key
=====================================================
Key code:
305C300D06092A864886F70D0101010500034B003048024100D6665EFEC14F48A5B42A413E2FACCAA9F02C77
2AEDC4911E76AAEE55BA49C4A0233D2D80504068BD9C892C0DD9EBBBC7EB8842ED61CDB418A29CA1362BB48C
190203010001

=====================================================
Time of Key pair created: 03:14:36  2000/04/06
Key name: Sysname_Server
Key type: RSA encryption Key
=====================================================
Key code:
```

```
307C300D06092A864886F70D0101010500036B003068026100A3B63F5B0E5470D9FE2005450342011FEDE2A9
24C71EB19E28D257E43EF7E531D7C37FBB157712A2F2AF0F5BAF3E60595496C5B3EAFF25BFB56F1E1CC7A700
4D0FF048654BFEADB21C5AF3E24FB0516393BFEEF65A83B7416F170886904C8BE30203010001
```

Create a DSA key pair.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[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.
Input the bits in the modulus[default = 1024]:
Generating keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+.........+............+............+...+.....+.............+..+...
...+................+.........+...+....+.......+.....+...........+.........+.
.......................+........+.........+.............+.....+...+..........
.............+.........+.........+..........+........+....+.................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
......
```

Display the public key information of the local DSA key pair.

```
[Sysname]display public-key local dsa public

=====================================================
Time of Key pair created: 03:17:33  2000/04/06
Key name:
Key type: DSA encryption Key
=====================================================
Key code:
3081F03081A806072A8648CE38040130819C0241008DF2A494492276AA3D25759BB06869CBEAC0D83AFB8D0C
F7CBB8324F0D7882E5D0762FC5B7210EAFC2E9ADAC32AB7AAC49693DFBF83724C2EC0736EE31C80291021500
C773218C737EC8EE993B4F2DED30F48EDACE915F0240626D027839EA0A13413163A55B4CB500299D5522956C
EFCB3BFF10F399CE2C2E71CB9DE5FA24BABF58E5B79521925C9CC42E9F6F464B088CC572AF53E6D788020343
0002406FBDE6C9BD578722585CDF4F3BFB31DD739865D1EA0312EDF2BAF4841C0A963E400640E46720681729
2CDFE5D91D86FDB9C3A16141E675E6FFC6C2577E660FF1
```

public-key local destroy

Syntax

public-key local destroy { **dsa** | **rsa** }

View

System view

Parameters

dsa: Specifies the DSA key pair.

rsa: Specifies the RSA key pair.

Description

Use the **public-key local destroy** command to destroy the key pairs generated for the current switch.

If the key pair does not exist, the system displays a message, telling you no such key pair exists.

Related commands: **public-key local create**.

Examples

Destroy the RSA key pairs of the current switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]public-key local destroy dsa
% Confirm to destroy these keys? [Y/N]:y
......
```

Destroy the DSA key pair of the current switch.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] public-key local destroy dsa
% Confirm to destroy these keys? [Y/N]:y
......
```

public-key local export rsa

Syntax

public-key local export rsa { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

Parameters

rsa: Specifies the host public key of the current switch's RSA key pair.

openssh: Specifies the format of the exported public key as OpenSSH.

ssh1: Specifies the format of the exported public key as SSH1.

ssh2: Specifies the format of the exported public key as SSH2.

filename: Name of the file for saving the host public key, a string of 1 to 142 characters. For file naming rules, refer to *File System Management Command*.

Description

Use the **public-key local export rsa** command to export the current switch's RSA key pair to a specified file.

If you specify a filename, the command exports the host public key to the specified file and saves the file; otherwise, the command displays the host public key on the screen.

Caution

- SSH1, SSH2, and OpenSSH are three public key formats. You can choose one as required. For example, if you want to export the RSA host public key to a file in the SSH1 format, use the **public-key local export rsa ssh1** *filename* command.
- The host public key displayed on the screen is in a format that is not transformed and cannot be used as the public key data for public key configuration.

Related commands: **public-key local create**, **rsa local-key-pair create**.

Examples

Generate 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.
Input the bits in the modulus[default = 1024]:
Generating keys...
..........................................++++++
......++++++
................++++++++
.....++++++++
.......
```

Display the host public key in the OpenSSH format.

```
[Sysname]public-key local export rsa openssh
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgMSPi+xIkHkAo6E9LwLKWN+eN9EqW/6FIYEIlVKcpIa0
6IT4eSyq4OldeiZ9WorOiDqX3ROo4FmaTR/QCSK3C9whE1qz/4soVL1eHDdgzQCumKKsJCVaM5OdZ2sdNbEnhLuc
s8ZrfTgEkDB1hmbgzuDpWPokPfkQDD+8dC+hkFVV rsa-key
```

Export the host public key in the format of OpenSSH and save the public key file as pub_ssh_file2.

```
[Sysname] public-key local export rsa openssh pub_ssh_file2
```

Export the host public key in the format of SSH1 and save the public key file as pub_ssh_file3.

```
[Sysname] public-key local export rsa ssh1 pub_ssh_file3
```

public-key local export dsa

Syntax

public-key local export dsa { **openssh** | **ssh2** } [*filename*]

View

System view

Parameters

dsa: Specifies the public key of the current switch's DSA key pair.

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.

filename: Name of the file for saving the public key, a string of 1 to 142 characters. For file naming rules, refer to *File System Management Command*.

Description

Use the **public-key local export dsa** command to export the current switch's DSA key pair to a specified file.

If you specify a filename, the command exports the public key to the specified file and saves it; otherwise, the command displays the public key on the screen.

Caution

- SSH2 and OpenSSH are two public key formats. You can choose one as required. For example, if you want to export the DSA host public key to a file in the SSH2 format, use the **public-key local export dsa ssh2** *filename* command.
- The host public key displayed on the screen is in a format that is not transformed and cannot be used as the public key data for public key configuration.

Related commands: **public-key local create**.

Examples

Generate a 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.
Input the bits in the modulus[default = 1024]:
Generating keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.....................+
..........+.............+............+...+.....+.............+..+......+...........
.....+.........+...+....+.......+.....+...........+.........+.....................
+........+.........+.............+.....+...+.....................+.........+.......
...+...........+........+....+.....................++++++++++++++++++++++++++++++++
++++++++++++++++*
.......
```

Display the public key in the SSH2 format.

```
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20000406"
AAAAB3NzaC1kc3MAAACA11cmLEWExEwhHxi9luXwYcTwpCP3/mtrhbNM73LOFKDTpSIv4Izs5lvmwmWFSIncHtvR
PsiydNqfdbomzLmHcjYCeH6SK6hEIfIsPInLmwb9YP4BlB3dd/5rEok9p27rwdEo2X8GeNdyK1NByFBvNYIUsWov
```

```
rEs2iVA4eBHH2jMAAAAUx3MhjHN+yO6ZO08t7TD0jtrOkV8AAACAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/Orp
bsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQe
y4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACA04Cd4ccxNjCMWzPAzZhj65GjyxExYS72XKWt
0S0AUs51ttRCqOHV/G8LUcdQ4pkp7XK6YGvxS0m1RPb9cIOMQZSYdHiXOq45zFA3Y8ylnWWF6EiuVUstjN8RC8Vt
nTzzIbihwmSSR0R9OEGi1vnxCdA1l5wDhuEYJMgq9ipVXLA=
---- END SSH2 PUBLIC KEY ----
```

Export the public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

View

System view

Parameters

keyname: Name of the public key, a string of 1 to 64 characters.

Description

Use the **public-key peer** command to enter public key view.

Use the **undo public-key peer** command to delete the configuration of peer public key.

After configuring this command, you enter public key view. You can use this command together with the **public-key-code begin** command to configure the peer public key. This public key configuration method requires that you obtain the public key in hexadecimal format in advance.

Note

Only the public key whose module is of 512 to 2,048 bits can be configured on the device currently.

Related commands: **public-key-code begin**, **public-key-code end**.

Examples

Enter public key view

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]public-key peer pub.ppk
PKEY public key view: return to System View with "peer-public-key end".
[Sysname-peer-public-key]
```

public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

View

System view

Parameters

keyname: Name of the public key , a string of 1 to 64 characters.

filename: Name of a public key file, a string of 1 to 142 characters. For file naming rules, refer to *File System Management Command*.

Description

Use the **public-key peer import sshkey** command to import a peer public key from the public key file.

Use the **undo public-key peer** command to remove the setting.

Note

- Only public key files in the format of SSH1, SSH2, or OpenSSH are supported.
- Currently, only public keys whose modules are in the range 512 to 2048 bits can be imported to the switch.
- You may use this command to configure an SSH peer's public key on the current switch. After you issue this command, the system will automatically identify the format of the public key, transforms the public key into the PKCS format, and saves the public key locally. This public key configuration method requires that the public key file be uploaded to the current switch through FTP or TFTP.

Examples

Configure the devices so that an SSH connection can be set up between the SSH server and an SSH client using publickey authentication. The following describes key configuration steps related to publickey authentication only.

On the SSH server, configure publickey authentication as the authentication mode for the client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh user client authentication-type publickey
```

On the SSH client, generate RSA key pairs and export the RSA host public key to a file.

```
<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.
```

```
Input the bits in the modulus[default = 1024]:
Generating keys...
.........................................++++++
......++++++
.................++++++++
.....++++++++
.......
[Sysname] public-key local export rsa ssh2 pub
```

Send the public key file of the SSH client to the SSH using FTP or TFTP. The configuration is omitted.

On the SSH server, import the SSH client's public key from the public key file, and then assign the public key to the SSH client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] public-key peer publick import sshkey pub
[Sysname] ssh user client assign publickey publick
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Parameters

None

Description

Use the **public-key-code begin** command to enter public key edit view.

Using the **public-key peer** command to enter public key view, and use the **public-key-code begin** command to enter the public key edit view. Then you can input the key by pasting the copied characters or pressing the keys on the keyboard. It must be a hexadecimal string that has been encoded complying with PKCS. Spaces and carriage returns are allowed between characters.

Related commands: **rsa peer-public-key**, **public-key peer**, **public-key-code end**.

Examples

Enter public key edit view and input a public key.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa peer-public-key Switch003
RSA public key view: return to System View with "peer-public-key end".
[Sysname-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[Sysname-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[Sysname-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[Sysname-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
```

```
[Sysname-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[Sysname-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[Sysname-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[Sysname-rsa-key-code] public-key-code end
[Sysname-rsa-public-key]
```

public-key-code end

Syntax

public-key-code end

View

Public key edit view

Parameters

None

Description

Use the **public-key-code end** command to return from public key edit view to public key view and save the public key you input.

After you use this command to end editing the public key, the system will check the validity of the public key before saving the key.

- If there is any illegal character in the key, your configuration fails. In this case, a prompt is displayed and the key is discarded.
- If the key is valid, it is saved in the local public key list.

Related commands: **rsa peer-public-key**, **public-key peer**, **public-key-code begin**.

Examples

Exit public key edit view and save the public key you input.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa peer-public-key Switch003
RSA public key view: return to System View with "peer-public-key end".
[Sysname-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[Sysname-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[Sysname-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[Sysname-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[Sysname-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[Sysname-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[Sysname-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[Sysname-rsa-key-code] public-key-code end
[Sysname-rsa-public-key]
```

rsa local-key-pair create

Syntax

rsa local-key-pair create

View

System view

Parameters

None

Description

Use the **rsa local-key-pair create** command to generate an RSA key pair for the current switch.

Note that:

- After entering this command, you will be prompted to provide the length of the key modulus. The length is in the range 512 to 2048 bits and defaults to 1024 bits. If the key pair already exists, the system will ask you whether you want to overwrite it.
- The configuration of this command can survive a reboot. You only need to configure it once.
- After the RSA key pair is generated, the **display rsa local-key-pair public** command displays two public keys (the host public key and server public key) when the switch is working in SSH1-compatible mode, but only one public key (the host public key) when the switch is working in SSH2 mode.

Related commands: **rsa local-key-pair destroy**, **display rsa local-key-pair public**.

Examples

Generate local RSA key pairs.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa local-key-pair create
The local-key-pair will be created.
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:
Generating keys...
.....................++++++
.......++++++
.................................++++++++
...++++++++
........Done!
```

Display the public keys of the current switch's RSA key pairs.

```
[Sysname] display rsa local-key-pair public

=====================================================
Time of Key pair created: 02:31:51  2000/04/09
Key name: Sysname_Host
```

```
Key type: RSA encryption Key
=====================================================
Key code:
308188
  028180
    F0C0EDA9 FA2E2FAC 4B16CA34 677F1861 A13E89BE
    6AAAC326 4E17268D EFADED1A FCA39047 52F18422
    B8C875DF 3626150D 4057EE12 371D5E62 57D34A16
    5045A403 FA805F72 B2780C9A 041ED99E 2841F600
    AB30DB10 821EF338 1FA54FE5 3DC79E46 74E45127
    3D4CA70F 253645DA 57524DC3 513BAC53 2C1B7F8F
    2481FA79 D4AA15C7
  0203
    010001

=====================================================
Time of Key pair created: 02:32:06  2000/04/09
Key name: Sysname_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    C9BEF5C8 1AF3E457 AD007039 DDB21785 28B0204F
    A9ED61A6 AD381860 9491B700 0286568F 4CAF27B1
    1B17B1A2 0D516E74 8DAFA6C1 0F71624B B8BE6FB2
    F550E7B9 BABD5B34 7D3E85C2 126B59DC 93BB4EA5
    6A147737 E9CE41EB 1B31171C 142902AF
  0203
    010001
```

rsa local-key-pair destroy

Syntax

rsa local-key-pair destroy

View

System view

Parameters

None

Description

Use the **rsa local-key-pair destroy** command to destroy the current switch's RSA key pair.

If the local RSA key pairs do not exist, the system displays a message, telling you no such key pairs exist.

Related commands: **rsa local-key-pair create**.

Examples

Destroy the current switch's RSA key pairs.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa local-key-pair destroy
% The local-key-pair will be destroyed.
% Confirm to destroy these keys? [Y/N]:y
.............Done!
```

rsa peer-public-key

Syntax

rsa peer-public-key *keyname*

undo rsa peer-public-key *keyname*

View

System view

Parameters

keyname: Name of the public key to be configured , a string of 1 to 64 characters.

Description

Use the **rsa peer-public-key** command to enter public key view.

Use the **undo rsa peer-public-key** command to remove the setting.

After using this command, you can use the **public-key-code begin** command to configure the peer public key. This public key configuration method requires that you obtain the peer public key in hexadecimal format in advance.

Note

Currently, the switch supports only public keys of 512 to 2048 bits.

Related commands: **public-key-code begin**, **public-key-code end**.

Examples

Enter Switch002 public key view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] rsa peer-public-key Switch002
RSA public key view: return to System View with "peer-public-key end".
[Sysname-rsa-public-key]
```

rsa peer-public-key import sshkey

Syntax

rsa peer-public-key *keyname* **import sshkey** *filename*

undo rsa peer-public-key *keyname*

View

System view

Parameters

keyname: Name of the public key to be configured, a string of 1 to 64 characters.

filename: Name of a public key file, a string of 1 to 142 characters. For file naming rules, refer to *File System Management Command*.

Description

Use the **rsa peer-public-key import sshkey** command to import a peer public key from the public key file.

Use the **undo rsa peer-public-key** command to remove the setting.

After execution of this command, the system automatically transforms the public key file into PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP/TFTP.

Note

- Only public key files in the format of SSH1 or SSH2 are supported.
- Currently, only public keys with the modulues being in the range 512 to 2048 bits can be imported to the switch.
- You may use this command to configure an SSH peer's public key on the current switch. After you issue this command, the system will automatically identify the format of the public key, transforms the public key into the PKCS format, and saves the public key locally. This public key configuration method requires that the public key file be uploaded to the current switch through FTP or TFTP.

Caution

The **rsa peer-public-key import sshkey** command can transform only RSA public keys. If you want DSA public keys to be transformed and configured automatically, use the **public-key peer import sshkey** command.

Examples

Transform the format of client public key file abc and configure a public key named 123.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] rsa peer-public-key 123 import sshkey abc
```

ssh authentication-type default

Syntax

ssh authentication-type default { all | password | password-publickey | publickey | rsa }

undo ssh authentication-type default

View

System view

Parameters

all: Specifies either the password authentication or the publickey authentication for SSH users.

password: Specifies the authentication mode for SSH users as password authentication.

password-publickey: Specifies that both the password and the publickey must be authenticated for SSH users.

publickey: Specifies the authentication mode for the SSH user as publickey (RSA key or DSA key) authentication.

rsa: Specifies the authentication mode for the SSH user as publickey (RSA key or DSA key) authentication. The authentication modes specified by the **rsa** keyword and **publickey** keyword are implemented in the same way.

Description

Use the **ssh authentication-type default** command to specify a default authentication mode for SSH users. After this command is configured, when an SSH user is added by using the **ssh user** command, the default authentication mode is adopted for the user if no authentication mode is specified by using the **ssh user authentication-type** command.

Use the **undo ssh authentication-type default** command to remove the specified default authentication mode. That is, no default authentication mode is specified for SSH users. In this case, when an SSH user is added, you must specify an authentication mode for the user at the same time.

By default, no default authentication mode is specified.

The differences between password authentication, publickey authentication, and password-publickey authentication are:

- Password authentication is vulnerable to attacks.
- Publickey authentication provides more secure SSH connections than password authentication does. The mode is easy to use and prevents illegal operations such as malicious password guess. After the configuration, the subsequent authentications are implemented automatically without asking you to enter the password.
- Password-publickey authentication takes the advantages of both password authentication and publickey authentication. An SSH user must pass both types of authentication before logging in. The combination of password and publickey authentications eliminates the vulnerability of the SSH server caused by the clients. You can use password-publickey authentication together with AAA for authentication and authorization of users.

Related commands: **display ssh user-information**.

Examples

Specify the publickey authentication as the default authentication mode.

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

Create an SSH user

```
[Sysname] ssh user user1
```

Display information about configured SSH users.

```
[Sysname] display ssh user-information
 Username            Authentication-type  User-public-key-name  Service-type
 user1               publickey            null                  stelnet
```

ssh client assign

Syntax

ssh client { *server-ip* | *server-name* } **assign** { **publickey** | **rsa-key** } *keyname*

undo ssh client { *server-ip* | *server-name* } **assign** { **publickey** | **rsa-key** }

View

System view

Parameters

server-ip: IP address of the server.

server-name: Name of the server, a string of 1 to 184 characters.

keyname: Name of the public key of the server, a string of 1 to 64 characters.

Note

Both the **publickey** and **rsa-key** keywords indicate specifying the publickey key. They are implemented with the same method.

Description

Use the **ssh client assign** command to specify the name of the public key of the server on the client so that the client can authenticate whether the server to be accessed is reliable.

Use the **undo ssh client assign** command to remove the mapping between the client and the public key of the server.

By default, a client does not have the name of the server's public key specified and it uses the IP address or host name that it used to log in to the SSH server as the public key name.

Note

If a client does not support first-time authentication, it will refuse to access any unauthenticated server. In this case, you need to configure the public key of the server on the client and associate the public key and the server so that the client can authenticate the server during login.

Caution

If a pair of SSH peers are both switches that support both DSA and RSA, you must configure the DSA public key of the server on the client.

Related command: **ssh client first-time enable**.

Examples

Specify the name of the DSA public key of the server (whose IP address is 192.168.0.1) as **pub.ppk** on the client.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh client 192.168.0.1 assign publickey pub.ppk
```

ssh client first-time enable

Syntax

ssh client first-time enable

undo ssh client first-time

View

System view

Parameters

None

Description

Use the **ssh client first-time enable** command to enable the client to run first-time authentication for the SSH server it accesses for the first time.

Use the **undo ssh client first-time** command to disable the client from running first-time authentication.

By default, the client is enabled to run first-time authentication.

Note that:

- With first-time authentication enabled, an SSH client that is not configured with the server's host public key can continue accessing the server when it accesses the server for the first time. The SSH server sends its host public key to the client automatically, and the client saves the key for use

in subsequent authentications. In this mode, the client cannot ensure the correctness of the SSH server's host public key.

- With first-time authentication disabled, you must configure the server's host public key and specify the public key name for authentication on the client in advance.

For details about first-time authentication, refer to corresponding section in *SSH Operation.*

Examples

Disable the client to run first-time authentication on an SSH client.

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

ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Parameters

times: Authentication retry times, in the range of 1 to 5.

Description

Use the **ssh server authentication-retries** command to set the authentication retry times for SSH connections. This configuration will take effect for all users logging in later.

Use the **undo ssh server authentication-retries** command to restore the default authentication retry times.

By default, the number of authentication retry times is 3.

 **Caution**

If you have used the **ssh user authentication-type** command to configure the authentication type of a user to **password-publickey**, you must set the authentication retry times to a number greater than or equal to 2 (so that the user can access the switch).

Related commands: **display ssh server**.

Examples

Set the authentication retry times to four.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh server authentication-retries 4
```

ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

View

System view

Parameters

None

Description

Use the **ssh server compatible-ssh1x enable** command to make the server compatible with SSH1.x clients.

Use the **undo ssh server compatible-ssh1x** command to make the server incompatible with SSH1.x clients.

By default, the server is compatible with SSH1.x clients.

Related commands: **display ssh server**.

Examples

Configure the server to be compatible with SSH1.x clients.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh server compatible-ssh1x enable
```

ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Parameters

hours: Interval to update the server keys, ranging from 1 to 24 (in hours).

Description

Use the **ssh server rekey-interval** command to set the interval to update the RSA server keys regularly.

Use the **undo ssh server rekey-interval** command to cancel the current configuration.

By default, the update interval is zero, which indicates the system does not update the server keys.

Caution

This command only takes effect on users whose client version is SSH1.x.

Related commands: **display ssh server**.

Examples

Configure to update the server's keys every 3 hours.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh server rekey-interval 3
```

ssh server timeout

Syntax

ssh server timeout *seconds*

undo ssh server timeout

View

System view

Parameters

seconds: Authentication timeout time, ranging from 1 to 120 (in seconds).

Description

Use the **ssh server timeout** command to set the authentication timeout time for SSH connections.

Use the **undo ssh server timeout** command to restore the default timeout time (that is, 60 seconds).

The configuration here will take effect at next login.

Related commands: **display ssh server**.

Examples

Set the authentication timeout time to 80 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh server timeout 80
```

ssh user

Syntax

ssh user *username*

undo ssh user *username*

View

System view

Parameters

username: SSH user name, a string of 1 to 184 characters. It cannot contain any of these characters: slash (/), backslash (\), colon (:), asterisk (*), question mark (?), less than sign (<), greater than sign (>), and the vertical bar sign (|). In addition, the @ sign can appear up to once, the username part (that is, the string before the @ sign) cannot be more than 55 characters, and the domain name part cannot be more than 128 characters.

Description

Use the **ssh user** command to create an SSH user.

Use the **undo ssh user** to delete a specified SSH user.

An SSH user is represented as a set of user attributes on the SSH server. This set is uniquely identified with the SSH username. When a user logs in to the SSH server from the SSH client, a username is required so that the server can looks up the database for matching the username. If a match is found, it authenticates the user using the authentication mode specified in the attribute set. If not, it tears down the connection.

 **Caution**

An SSH user created with this command uses the default authentication type specified by the **ssh authentication-type default** command. If no default authentication type is specified for SSH users, you need to use the **ssh user authentication-type** command to create an SSH user and specify an authentication mode for the user.

 **Note**

An SSH user is created on an SSH server for the purpose of specifying the authentication type, the SSH service type, and the public key for the SSH user. An existing SSH user will be removed automatically if it has none of the authentication type, the SSH service type, and the public key configured.

Related commands: **ssh authentication-type default**, **ssh user authentication-type**.

Examples

Specify the default authentication type as password authentication. Create an SSH user with the name “abc”.

```
<Sysname> system-view
Enter system view, return to user view with Ctrl+Z.
[Sysname] ssh authentication-type default password
[Sysname] ssh user abc
```

Display the SSH user information.

```
[Sysname] display ssh user-information abc
 Username            Authentication-type  User-public-key-name  Service-type
```

```
abc                 password            null                stelnet
```

ssh user assign

Syntax

ssh user *username* **assign** { **publickey** | **rsa-key** } *keyname*

undo ssh user *username* **assign** { **publickey** | **rsa-key** }

View

System view

Parameters

username: SSH user name, a string of 1 to 184 characters. It cannot contain any of these characters: slash (/), backslash (\), colon (:), asterisk (*), question mark (?), less than sign (<), greater than sign (>), and the vertical bar sign (|). In addition, the @ sign can appear up to once, the username part (that is, the string before the @ sign) cannot be more than 55 characters, and the domain name part cannot be more than 128 characters.

keyname: Name of a public key, a string of 1 to 64 characters.

Description

Use the **ssh user assign** command to assign an existing public key to a specified SSH user on the SSH server side.

Use the **undo ssh user assign** command to remove the association.

The public key of the client is subject to the one assigned last time.

The new public key takes effect when the user logs in next time.

Note

- On an SSH server, you need to assign a public key to each SSH user using publickey authentication.
- Both **publickey** and **rsa-key** indicate specifying the publickey key. They are implemented with the same method.

Related commands: **display ssh user-information**.

Examples

Assign a public key named 127.0.0.1 to SSH client 1.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]ssh user 1 assign publickey 127.0.0.1
```

Display SSH user information.

```
[Sysname] display ssh user-information 1
 Username            Authentication-type  User-public-key-name  Service-type
```

```
1                publickey          127.0.0.1          stelnet
```

ssh user authentication-type

Syntax

ssh user *username* **authentication-type** { **all** | **password** | **password-publickey** | **publickey** | **rsa** }

undo ssh user *username* **authentication-type**

View

System view

Parameters

username: SSH user name, a string of 1 to 184 characters. It cannot contain any of these characters: slash (/), backslash (\), colon (:), asterisk (*), question mark (?), less than sign (<), greater than sign (>), and the vertical bar sign (|). In addition, the @ sign can appear up to once, the username part (that is, the string before the @ sign) cannot be more than 55 characters, and the domain name part cannot be more than 128 characters.

all: Specifies that the authentication mode for the SSH user can be either password authentication or publickey authentication.

password: Specifies the authentication mode for the SSH user as password authentication.

password-publickey: Specifies the authentication mode for the SSH user as password and publickey.

publickey: Specifies the authentication mode for the SSH user as publickey (RSA key or DSA key) authentication.

rsa: Specifies the authentication mode for the SSH user as publickey (RSA key or DSA key) authentication. The authentication modes specified by the **rsa** keyword and **publickey** keyword are implemented in the same way

---

Note

For the **password-publickey** authentication type:

- SSH1 client users can access the switch as long as they pass one of the two authentications.
- SSH2 client users can access the switch only when they pass both the authentications.

Description

Use the **ssh user authentication-type** command to specify the authentication mode for SSH users on the server.

Use the **undo ssh user authentication-type** command to remove the configuration.

The differences between password authentication, publickey authentication, and password-publickey authentication are:

- Password authentication is vulnerable to attacks.
- Publickey authentication provides more secure SSH connections than password authentication does. The mode is easy to use and prevents illegal operations such as malicious password guess.

After the configuration, the subsequent authentications are implemented automatically without asking you to enter the password.

- Password-publickey authentication takes the advantages of both the password authentication and publickey authentication. An SSH user must pass both types of authentication before logging in. The combination of password and publickey authentications eliminates the vulnerability of the SSH server caused by the clients. You can use password-publickey authentication together with AAA for authentication and authorization of users.

Caution

You need to specify the authentication mode for an SSH user. Otherwise, the user will not be able to log in to the SSH server.

Related commands: **display ssh user-information**.

Examples

Specify the publickey authentication for SSH users.

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]ssh user kk authentication-type publickey
```

Display the SSH user information.

```
[Sysname] display ssh user-information kk
 Username            Authentication-type  User-public-key-name  Service-type
 kk                  publickey            null                  stelnet
```

ssh user service-type

Syntax

ssh user *username* **service-type** { **stelnet** | **sftp** | **all** }

undo ssh user *username* **service-type**

View

System view

Parameters

username: SSH user name, a string of 1 to 184 characters. It cannot contain any of these characters: slash (/), backslash (\), colon (:), asterisk (*), question mark (?), less than sign (<), greater than sign (>), and the vertical bar sign (|). In addition, the @ sign can appear up to once, the username part (that is, the string before the @ sign) cannot be more than 55 characters, and the domain name part cannot be more than 128 characters.

stelnet: Specifies the service type of secure Telnet..

sftp: Specifies the service type as secure FTP..

all: Specifies both secure Telnet and secure FTP.

Description

Use the **ssh user service-type** command to configure service type for a user so that the user can access specified service(s).

Use the **undo ssh user service-type** command to remove the service type specified for an SSH user.

The default service type for an SSH user is **stelnet**.

Related commands: **display ssh user-information**.

Examples

Specify that user kk can access SFTP service.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh user kk service-type sftp
```

Display the SSH user information.

```
[Sysname] display ssh user-information kk
 Username            Authentication-type  User-public-key-name  Service-type
 kk                  publickey            null                  sftp
```

ssh2

Syntax

ssh2 { *host-ip* | *host-name* } [*port-num*] [**identity-key** { **dsa** | **rsa** } | **prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **3des** | **des** | **aes128** } | **prefer_stoc_cipher** { **3des** | **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *

View

System view

Parameters

host-ip: Server IP address.

host-name: Server name, a string of 1 to 20 characters.

port-num: Server port number. It is in the range of 0 to 65,535 and defaults to 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **rsa**.

prefer_kex: Specifies the preferred key exchange algorithm. You can select one from the following two algorithms.

- **dh_group1**: Diffie-Hellman-group1-sha1 key exchange algorithm. It is the default algorithm.
- **dh_exchange_group**: Diffie-Hellman-group-exchange-sha1 key exchange algorithm.

prefer_ctos_cipher: Specifies the preferred client-to-server encryption algorithm, which is AES128 by default.

prefer_stoc_cipher: Specifies the preferred server-to-client encryption algorithm, which is AES128 by default.

- **3des**: 3DES_cbc encryption algorithm. Support for this keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not.
- **des**: DES_cbc encryption algorithm.
- **aes128**: AES_128 encryption algorithm.

prefer_ctos_hmac: Specifies the preferred client-to-server HMAC (Hash-based message authentication code) algorithm, which is SHA1_96 by default.

prefer_stoc_hmac: Specifies the preferred server-to-client HMAC algorithm, which is SHA1_96 by default.

- **sha1**: HMAC-SHA1 algorithm.
- **sha1_96**: HMAC-SHA1-96 algorithm.
- **md5**: HMAC-MD5 algorithm.
- **md5_96**: HMAC-MD5-96 algorithm.

 **Note**

- DES (data encryption standard) is a standard data encryption algorithm.
- AES (advanced encryption standard) is an advanced encryption standard algorithm.

Description

Use the **ssh2** command to start the SSH client to establish a connection with an SSH server, and at the same time specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client.

Note that when logging into the SSH server using publickey authentication, an SSH client needs to read its own private key for authentication. As two algorithms (RSA or DSA) are available, the **identity-key** keyword must be used to specify one algorithm in order to get the correct private key.

Examples

Log into SSH server 10.214.50.51 with:

- **dh_exchange_group** as the preferred key exchange algorithm,
- **aes128** as the preferred server-to-client encryption algorithm,
- **md5** as the preferred client-to-server HMAC algorithm, and
- **sha1_96** as the preferred server-to-client HMAC algorithm.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh2 10.214.50.51 prefer_kex dh_exchange_group prefer_stoc_cipher aes128
prefer_ctos_hmac md5 prefer_stoc_hmac sha1_96
```

ssh2 source-interface

Syntax

ssh2 source-interface *interface-type interface-number*

undo ssh2 source-interface

View

System view

Parameters

interface-type: Source interface type.

interface-number: Source interface number.

Description

Use the **ssh2 source-interface** command to specify a source interface for the SSH client. If the specified interface does not exist, the command fails.

Use the **undo ssh2 source-interface** command to cancel the source interface setting. You can configure an IP address by specifying the corresponding interface for the client to use to access the SSH server. This improves the service manageability when the SSH client has multiple IP addresses and interfaces.

Examples

Specify source interface Vlan-interface 1 for the SSH client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh2 source-interface Vlan-interface 1
```

ssh2 source-ip

Syntax

ssh2 source-ip *ip-address*

undo ssh2 source-ip

View

System view

Parameters

ip-address: Source IP address.

Description

Use the **ssh2 source-ip** command to specify a source IP address for the SSH client. If the specified IP address is not an address of the device, the command fails.

Use the **undo ssh2 source-ip** command to cancel the source IP address setting.

You can specify a souce IP address for the client to use to access the SSH server. This improves the service manageability when the SSH client has multiple IP addresses.

Examples

Specify source IP address 192.168.1.1 for the SSH client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh2 source-ip 192.168.1.1
```

ssh-server source-interface

Syntax

ssh-server source-interface *interface-type interface-number*

undo ssh-server source-interface

View

System view

Parameters

interface-type: Source interface type.

interface-number: Source interface number.

Description

Use the **ssh-server source-interface** command to specify a source interface for the SSH server. If the specified interface does not exist, the command fails.

Use the **undo ssh-server source-interface** command to cancel the source interface setting.

You can specify a source interface that corresponds to the IP address for the SSH server to provide SSH access services for the clients. In this way, the SSH clients can only access the SSH server using the IP address of the specified interface as the destination. This improves the service manageability when the SSH server has multiple IP addresses and interfaces,

Examples

Specify Vlan-interface 1 as the source interface of the SSH server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh-server source-interface Vlan-interface 1
```

ssh-server source-ip

Syntax

ssh-server source-ip *ip-address*

undo ssh-server source-ip

View

System view

Parameters

ip-address: IP address to be set as the source IP address.

Description

Use the **ssh-server source-ip** command to specify a source IP address for the SSH server. If the specified IP address is not an IP address of the device, the command fails.

Use the **undo ssh-server source-ip** command to cancel the source IP address setting.

You can configure a source IP address for the SSH server to provide SSH access service for the SSH clients. In this way, the SSH clients can only access the SSH server using the specified IP address as the destination. This improves the service manageability when the SSH server has multiple IP addresses.

Examples

Specify source IP address 192.168.0.1 for the SSH server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ssh-server source-ip 192.168.0.1
```

Table of Contents

1 File System Management Configuration Commands

Note

3com switches 4200G allow you to input a file path and file name in one of the following ways:

- In universal resource locator (URL) format and starting with “unit1>flash:/”. or “flash:/” This method is used to specify a file in the current Flash memory. For example, the URL of a file named **text.txt** in the root directory of the switch is **unit1>flash:/text.txt** or **flash:/text.txt**.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory. For example, to access file text.txt in the current directory, you can directly input the file name **text.txt** as the file URL.

File System Configuration Commands

Note

Note to limit the lengths of device name, directory name, file path and file name within the following ranges regulated for the switch.

- A directory name should be no more than 91 characters.
- A file name plus its local path name should be no more than 127 characters.
- A device name should be no more than 14 characters.
- A file name plus its complete path name should be no more than 142 characters.

cd

Syntax

cd *directory*

View

User view

Parameter

directory: Target directory.

Description

Use the **cd** command to enter a specified directory on the Ethernet switch.

The default directory when a user logs onto the switch is the root directory of Flash memory.

Example

Enter the directory named test from the root directory.

```
<Sysname> cd test
```

Return to the upper directory. Note that keyword **cd** is followed by a space.

```
<Sysname> cd ..
```

After modifying the working directory using the **cd** command, you can use the **pwd** command to display the current working directory.

copy

Syntax

copy *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file.

Description

Use the **copy** command to copy a file.

If the *fileurl-dest* argument identifies an existing file, the existing file will be overwritten after the command is executed successfully.

If the path, rather than the name of the target file is specified, the source file name is used as the target file name by default.

Example

Copy file **config.cfg** from the root directory to directory **test**, and save the file using name **1.cfg**.

```
<Sysname> copy flash:/config.cfg flash:/test/1.cfg
Copy unit1>flash:/config.cfg to unit1>flash:/test/1.cfg?[Y/N]:y
...
%Copy file unit1>flash:/config.cfg to unit1>flash:/test/1.cfg...Done.
```

Copy file **config.cfg** from the root directory to directory **test**, and save the file using the original file name.

```
<Sysname> copy flash:/config.cfg flash:/test
Copy unit1>flash:/config.cfg to unit1>flash:/test/config.cfg?[Y/N]:y
...
%Copy file unit1>flash:/config.cfg to unit1>flash:/test/config.cfg...Done.
```

delete

Syntax

delete [**/unreserved**] *file-url*

delete { **running-files** | **standby-files** } [**/unreserved**]

View

User view

Parameter

/unreserved: Specifies to delete a file completely.

file-url: Path name or file name of a file in the Flash memory. You can use the * character in this argument as a wildcard. For example, the **delete** *.txt command deletes all the files with txt as their extensions.

running-files: Specifies to delete all the files with the main attribute.

standby-files: Specifies to delete all the files with the backup attribute.

Description

Use the **delete** command to delete a specified file from the Flash memory on a switch.

If you execute the **delete** command with the **/unreserved** keyword specified, the specified file is permanently deleted. That is, the file cannot be restored. If you execute the **delete** command without the **/unreserved** keyword, the specified file is removed to the recycle bin, and you can use the **undelete** command to restore it.

You can delete files based on file attribute.

- If you execute the **delete running-files** command, all the files with the main attribute will be deleted.
- If you execute the **delete standby-files** command, all the files with the backup attribute will be deleted.

For a file that has both the main and backup attributes:

- The **delete running-files** command only deletes its main attribute instead of the file itself.
- The **delete standby-files** command only deletes its backup attribute instead of the file itself.

When you use the **delete running-files** or **delete standby-files** command, you will be prompted to confirm whether to delete all files with the main/backup attribute. If you choose yes, the corresponding files are deleted. If you choose no, the system will further to prompt you to confirm the following items orderly:

1) Delete the image files with the main/backup attribute?
2) Delete the configuration files with the main/backup attribute?
3) Delete the Web files with the main/backup attribute?

The corresponding messages are displayed as follows:

```
Delete the running image file? [Y/N]:
Delete the running config file? [Y/N]:
Delete the running web file? [Y/N]:

Delete the backup image file? [Y/N]:
```

```
Delete the backup config file? [Y/N]:
Delete the backup web file? [Y/N]:
```

The corresponding files will be deleted after you choose yes.

Caution

For deleted files whose names are the same, only the latest deleted file is stored in the recycle bin and can be restored.

Example

Delete the file **test/test.txt**.

```
<Sysname> delete test/test.txt
Delete unit1>flash:/test/test.txt?[Y/N]:y
.
%Delete file unit1>flash:/test/test.txt...Done.
```

Delete the configuration files with the backup attribute in the Flash.

```
<Sysname> delete standby-files
Delete all the backup files? [Y/N]:n
Delete the backup image file? [Y/N]:n
Delete the backup config file? [Y/N]:y
Delete the backup web file? [Y/N]:n
Start deleting ...
Deleting ... done
```

dir

Syntax

dir [***/all***] [*file-url*]

View

User view

Parameter

/all: Specifies to display the information about all the files, including those stored in the recycle bin.

file-ur: Path name or the name of a file in the Flash memory. You can use the * character as a wildcard. For example, the **dir** *.txt command displays the information about all the files with the extension of txt in the current directory.

Description

Use the **dir** command to display the information about the specified files or directories in the Flash memory on a switch.

- If executed with the **/all** keyword, the command will display information about all files, including the files in the recycle bin. If executed without the **/all** keyword, the command will not display the files in the recycle bin.
- If executed with the *file-url* argument, the command will display information about files and folders in the specified directory. If executed without the *file-url* argument, the command will display information about files and folders in the current working directory.

In the output information, files with the main, backup or main/backup attribute are tagged with special characters:

- main: (*)
- backup: (b)
- main/backup: (*b)

Note

In the output information of the **dir /all** command, deleted files (that is, those in the recycle bin) are embraced in brackets. The displayed directory of a deleted file is the directory to which the file belongs before it is deleted.

Example

Display the information about all the files (including the files in the recycle bin) in the root directory of the file system.

```
<Sysname> dir /all
Directory of unit1>flash:/

   1 (*)   -rw-   3579326  Mar 28 2007 10:51:22   switch.bin
   2 (*)   -rw-      1235  Apr 03 2000 16:04:52   basic.cfg
   3       -rw-    140709  Apr 04 2000 21:31:08   cmdtree_b01d015.txt
   4       -rw-      1235  Apr 04 2000 23:03:08   test.txt
   5       drw-         -  Apr 04 2000 23:04:21   test
   6       -rw-      1235  Apr 04 2000 23:05:41   [1.cfg]

15367 KB total (3590 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

Display the information about all the files whose names begin with the character t (including those in the recycle bin) in the local directory unit1>flash:/test/.

```
<Sysname> dir /all test/t*
Directory of unit1>flash:/test/

   1       -rw-      1235  Apr 04 2000 23:08:28   test.txt

15367 KB total (3590 KB free)
```

```
(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

execute

Syntax

execute *filename*

View

System view

Parameter

filename: Batch file, with the extension .bat.

Description

Use the **execute** command to execute the specified batch file. Executing a batch file is to execute a set of commands in the batch file one by one.

Note that:

- A batch file cannot contain any invisible character. If any invisible character is found, the system will abort the execution of the batch file, that is, the remaining commands in the batch file will not be executed, but the executed operations will not be cancelled.
- Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.
- Each configuration command in a batch file must be a standard configuration command, meaning that the configuration information can be displayed with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

Example

Execute the batch file named test.bat under the directory flash:/.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] execute test.bat
<Sysname>
....
%Created dir unit1>flash:/test3.
```

file prompt

Syntax

file prompt { **alert** | **quiet** }

View

System view

Parameter

alert: Specifies to prompt for confirmation before performing file-related operations that have potential risks.

quiet: Specifies to disable prompts for file-related operations.

Description

Use the **file prompt** command to configure the prompt mode for file-related operations.

By default, alert mode is used, by which a switch prompts for confirmation before performing file-related operations that have potential risks.

If you set the prompt mode of the file-related operations to **quiet**, the switch does not prompt for confirmation before performing file-related operations. In this case, the system is more likely to be damaged due to some maloperations. For example:

- If the prompt mode is set to **alert**, the following messages will be displayed when you delete a file:

```
<Sysname> delete flash:/te.txt
Delete unit1>flash:/te.txt?[Y/N]:y
......
%Delete file unit1>flash:/te.txt...Done.
```

The system waits for you to confirm for 30 seconds. If you do not input any confirmation in 30 seconds, the system cancels this file operation, as shown in the following:

```
<Sysname> delete flash:/tt.txt
Delete unit1>flash:/tt.txt?[Y/N]:
<Sysname>
```

- If the prompt mode is set to **quiet**, the following messages will be displayed when you delete a file:

```
<Sysname> delete flash:/te.txt
....
%Delete file unit1>flash:/te.txt...Done.
```

Example

Set the prompt mode to **quiet** for file-related operations.

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

fixdisk

Syntax

fixdisk *device*

View

User view

Parameter

device: Name of a device which must be “unit1>flash:” or “flash:” for the 3com switch 4200G.

Description

Use the **fixdisk** command to restore space on the Flash memory.

In case that space on the Flash memory may become unavailable for reasons such as abnormal operations, you can run this command to restore the space.

Example

Restore space on the Flash memory.

```
<Sysname> fixdisk unit1>flash:
Fixdisk flash: may take some time to complete.
%Fixdisk unit1>flash: completed.
```

format

Syntax

format *device*

View

User view

Parameter

device: Name of a device which must be “unit1>flash:” or “flash:” for the 3com switch 4200G.

Description

Use the **format** command to format the Flash memory.

 **Caution**

The format operation clears all the files on the Flash memory, and the operation is irretrievable.

Example

Format the Flash memory.

```
<Sysname>format unit1>flash:
All data on unit1>flash: will be lost , proceed with format ? [Y/N]:y
.............................
%Format unit1>flash: completed.
```

mkdir

Syntax

mkdir *directory*

View

User view

Parameter

directory: Name of a directory.

Description

Use the **mkdir** command to create a subdirectory in the specified directory of a Flash memory.

Note that:

- The name of the subdirectory to be created must be unique under the specified directory. Otherwise, you will fail to create the subdirectory under the directory.
- To use this command to create a subdirectory, the specified directory must exist. For instance, to create subdirectory **flash:/test/mytest**, the **test** directory must exist. Otherwise, you will fail to create the subdirectory.

Example

Create a directory in the current directory, with the name being **test**.

```
<Sysname> mkdir test
....
%Created dir unit1>flash:/test.
```

Create subdirectory **mytest** in the directory **test**.

```
<Sysname> mkdir test/mytest
..
%Created dir unit1>flash:/test/mytest.
```

more

Syntax

more *file-url*

View

User view

Parameter

file-url: Path name or file name of a file in the Flash memory.

Description

Use the **more** command to display the contents of a specified file.

Currently, the file system only supports to display the contents of text files.

Example

Display the content of the file named test.txt.

```
<Sysname> more test.txt
AppWizard has created this test application for you.
This file contains a summary of what you will find in each of the files that make up your
test application.
Test.dsp
```

```
This file (the project file) contains information at the project level and is used to build
a single project or subproject. Other users can share the project (.dsp) file, but they should
export the makefiles locally.
```

Display the content of the file testcfg.cfg.

```
<Sysname> more testcfg.cfg

#
 sysname Sysname
#
 configure-user count 5
#
vlan 2
#
return
<Sysname>
```

move

Syntax

move *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file.

Description

Use the **move** command to move a file to a specified directory.

If the target file name is the same as an existing file, the existing file will be overwritten after the command is executed successfully.

If the path, rather than the name of the target file is specified, the source file name is used as the target file name by default.

Example

Move the file named 1.txt from unit1>flash:/ to unit1>flash:/a/, with the name unchanged.

```
<Sysname>move unit1>flash:/1.txt unit1>flash:/a/
Move unit1>flash:/1.txt to unit1>flash:/a/1.txt?[Y/N]:y
.
%Moved file unit1>flash:/1.txt to unit1>flash:/a/1.txt.
```

Move the file unit1>flash:/22.txt to unit1>flash:/test/, and overwrite the file in the directory unit1>flash:/test.

```
<Sysname>move 22.txt unit1>flash:/test
Move unit1>flash:/22.txt to unit1>flash:/test/22.txt?[Y/N]:y
The file unit1>flash:/test/22.txt exists. Overwrite it?[Y/N]:y
```

```
The file will be permanently deleted from flash, please wait.
....
%Moved file unit1>flash:/22.txt to unit1>flash:/test/22.txt.
```

pwd

Syntax

pwd

View

User view

Parameter

None

Description

Use the **pwd** command to display the current working path of the login user.

Example

Display the current working path.

```
<Sysname> pwd
unit1>flash:
```

rename

Syntax

rename *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Original path name or file name of a file in the Flash memory.

fileurl-dest: Target path name or file name.

Description

Use the **rename** command to rename a file or a directory.

If the target file name or directory name is the same with any existing file name or directory name, you will fail to perform the rename operation.

Example

Rename the file named config.txt to config.bak.

```
<Sysname>rename config.txt config.bak
Rename unit1>flash:/config.txt to unit1>flash:/config.bak?[Y/N]:y
.
%Renamed file unit1>flash:/config.txt to unit1>flash:/config.bak.
```

reset recycle-bin

Syntax

reset recycle-bin [*file-url*] [**/force**]

View

User view

Parameter

file-url: Path name or file name of a file in the Flash memory. This argument supports the wildcard “*”. For example, *.txt means all the files with an extension of txt.

/force: Specifies not to prompt for confirmation before deleting files.

Description

Use the **reset recycle-bin** command to permanently delete the files in the recycle bin in the current directory.

Use the **reset recycle-bin** *file-url* command to permanently delete the files in the recycle bin in the specified directory.

By default, the file operation reminding mode is **alert**, meaning that when you clear the files in the recycle bin on the local unit, the system will ask for your confirmation for each file you want to delete. However, if you specify the /**force** keyword in the command, the system will not ask for your confirmation.

The files deleted by the **delete** command without the **/unreserved** keyword are moved to the recycle bin. To delete them permanently, you can use the **reset recycle-bin** command.

Example

There are three files **flash:/a.cfg**, **flash:/b.cfg**, and **flash:/test/c.cfg** in the recycle bin. Permanently delete file **flash:/a.cfg** and **flash:/b.cfg**.

- Display all the files in the recycle bin in directory **flash:**.

```
<Sysname> dir /all
Directory of flash:/

   0     -rwh      3080  Apr 26 2000 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2000 13:45:36   config.cfg
   2     -rw-   4036197  May 14 2000 10:13:18   main.bin
   3     -rw-      2386  Apr 26 2000 13:30:30   back.cfg
   4     drw-         -  May 08 2000 09:49:25   test
   5     -rwh       716  Apr 24 2007 16:17:30   hostkey
   6     -rwh       572  Apr 24 2007 16:17:44   serverkey
   7     -rw-      2386  May 08 2000 11:14:20   [a.cfg]
   8     -rw-      3608  Dec 03 2007 17:29:30   [b.cfg]

15367 KB total (1930 KB free)
```

//The above information indicates that in directory **flash:**, there are two files **a.cfg** and **b.cfg** in the recycle bin.

- Delete the files in directory **flash:** that are already in the recycle bin.

```
<Sysname> reset recycle-bin
Clear flash:/~/a.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
....
%Cleared file flash:/~/a.cfg.
Clear flash:/~/b.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
......
%Cleared file flash:/~/b.cfg...
```

- In directory **flash:**, check whether all the files in the recycle bin are deleted.

```
<Sysname> dir /all
Directory of flash:/

   0     -rwh      3080  Apr 26 2000 16:41:43   private-data.txt
   1     -rw-      2416  Apr 26 2000 13:45:36   config.cfg
   2     -rw-   4036197  May 14 2000 10:13:18   main.bin
   3     -rw-      2386  Apr 26 2000 13:30:30   back.cfg
   4     drw-         -  May 08 2000 09:49:25   test
   5     -rwh       716  Apr 24 2007 16:17:30   hostkey
   6     -rwh       572  Apr 24 2007 16:17:44   serverkey

15367 KB total (1934 KB free)
```

// The above information indicates that file **flash:/a.cfg** and **flash:/b.cfg** are deleted permanently.

- In directory **flash:/test**, see whether the file in the recycle bin is deleted or not.

```
<Sysname> cd test
<Sysname> dir /all
Directory of flash:/test/

   0     drw-         -  Dec 03 2007 18:19:09   subtest
   1     -rw-      2386  Dec 03 2007 18:43:41   [c.cfg]

15367 KB total (1934 KB free)
```

// The above information indicates that file **flash:/test/c.cfg** in directory **flash:/test** is not deleted and is still in the recycle bin.

rmdir

Syntax

rmdir *directory*

View

User view

Parameter

directory: Name of a directory.

Description

Use the **rmdir** command to delete a directory.

As only empty directories can be deleted, you need to clear a directory before deleting it.

Example

Delete the directory named dd.

```
<Sysname> rmdir dd
Rmdir unit1>flash:/dd?[Y/N]:y
....
%Removed directory unit1>flash:/dd.
```

undelete

Syntax

undelete *file-url*

View

User view

Parameter

file-url: Path name or file name of a file in the Flash memory.

Description

Use the **undelete** command to restore a deleted file from the recycle bin.

If the name of the file to be restored is the same as that of an existing file, the existing file will be overwritten after the command is executed successfully.

Example

Restore the deleted file named sample.bak.

```
<Sysname> undelete sample.bak
Undelete unit1>flash:/sample.bak ?[Y/N]:y
% Undeleted file unit1>flash:/sample.bak.
```

File Attribute Configuration Commands

boot attribute-switch

Syntax

boot attribute-switch { **all** | **app** | **configuration** | **web** }

View

User view

Parameter

all: Specifies all the files, including app files, configuration files and Web files.

app: Specifies app files.

configuration: Specifies configuration files.

web: Specifies Web files.

Description

Use the **boot attribute-switch** command to switch between the main and backup attribute for all the files or a specified type of files. That is, change a file with the main attribute to one with the backup attribute, or vice versa.

Example

Switch the attributes of all the files.

```
<Sysname> boot attribute-switch all
 The boot, web and configuration file's backup-attribute and main-attribute will exchange.
 Are you sure? [Y/N] y
 The boot, web and configuration file's backup-attribute and main-attribute exchanged successfully on unit 1!
```

boot boot-loader

Syntax

boot boot-loader *file-url*

View

User view

Parameter

file-url: Path or the name of the app file in the Flash memory, a string comprising 1 to 64 characters.

Description

Use the **boot boot-loader** command to configure an app file of the device to be with the main attribute. The app file specified by this command becomes the main startup file when the device starts up next time.

Example

Configure the file named boot.bin to be the main startup file of the device.

```
<Sysname> boot boot-loader boot.bin
 The specified file will be booted next time on unit 1!
```

boot boot-loader backup-attribute

Syntax

boot boot-loader backup-attribute *file-url*

View

User view

Parameter

file-url: Path or the name of the app file in the Flash memory, a string comprising 1 to 64 characters.

Description

Use the **boot boot-loader backup-attribute** command to configure an app file of the device to be with the backup attribute. The app file specified by this command becomes the backup startup file when the device starts up next time. When the main startup file is unavailable, the backup startup file is used to start the switch.

Example

Configure the file named backup.bin to be the backup startup file of the device.

```
<Sysname> boot boot-loader backup-attribute backup.bin
 Set boot file backup-attribute successfully on unit 1!
```

boot web-package

Syntax

boot web-package *webfile* { **backup** | **main** }

View

User view

Parameter

webfile: Name of a Web file, a string comprising 5 to 127 characters (including the extension .web).

main: Specifies the file to be with the main attribute.

backup: Specifies the file to be with the backup attribute.

Description

Use the **boot web-package** command to configure a Web file in the device to be with the main or backup attribute.

Caution

- The configuration of the main or backup attribute for a Web file takes effect immediately without restarting the device.
- After you upgrade a Web file, you need to specify the new Web file in the Boot menu after restarting the switch or specify a new Web file by using the **boot web-package** command. Otherwise, the Web server cannot function normally.

Related commands: **display web package**

Example

Configure the Web file named boot.web to be with the main attribute.

```
<Sysname> boot web-package boot.web main
```

display boot-loader

Syntax

display boot-loader [**unit** *unit-id*]

View

Any view

Parameter

unit *unit-id*: Specifies the unit ID of a switch. You cannot choose any other number except 1 for the 3com switch 4200G.

Description

Use the **display boot-loader** command to display the information about the APP startup files of the device. Displayed information includes the current app startup file name, and the main and backup app startup files to be used when the switch starts up next time.

Example

Display the information about the app startup files.

```
<Sysname> display boot-loader unit 1
 Unit 1
   The current boot app is: switch.bin
   The main boot app is:     switch.bin
   The backup boot app is:   switchbak.bin
```

display web package

Syntax

display web package

View

Any view

Parameter

None

Description

Use the **display web package** command to display information about the Web file used by the device, including the name of the currently used Web file, and the name of the Web files with the main and backup attributes used for next startup.

Example

Display information about the Web file used by the device.

```
<Sysname>display web package
The current using web package is: flash:/http3.1.5-0040.web
The main web package is: unit1>flash:/http3.1.5-0040.web
The backup web package is: unit1>flash:/
```

startup bootrom-access enable

Syntax

startup bootrom-access enable

undo startup bootrom-access enable

View

User view

Parameter

None

Description

Use the **startup bootrom-access enable** command to specify a switch to prompt users to use customized password to enter the BOOT menu.

Use the **undo startup bootrom-access enable** command to disable the above function.

By default, users have to use customized passwords to enter the BOOT menu.

You can use the **display startup** command in the *Configuration File Management* part of the manual to view the execution results of these two commands.

Example

Specify to prompt users to use customized passwords to enter the BOOT menu.

```
<Sysname> startup bootrom-access enable
<Sysname> display startup
UNIT 1:
  Current Startup saved-configuration file:          flash:/config.cfg
  Next main startup saved-configuration file:        flash:/config.cfg
  Next backup startup saved-configuration file:      NULL
  Bootrom-access enable state:                       enabled
```

Table of Contents

1 FTP and SFTP Configuration Commands

FTP Server Configuration Commands

display ftp-server

Syntax

display ftp-server

View

Any view

Parameters

None

Description

Use the **display ftp-server** command to display the FTP server-related settings of a switch when it operates as an FTP server, including startup status, number of users, and so on.

You can use this command to verify FTP server-related configurations.

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

Examples

Display the FTP server-related settings of the switch (assuming that the switch is operating as an FTP server).

```
<Sysname> display ftp-server
   FTP server is running
   Max user number       1
   User count            0
   Timeout value(in minute)       30
```

Table 1-1 display ftp-server command output description

Field	Description
FTP server is running	The FTP server is started. If the FTP server is not started, “% FTP server has been stopped” will be displayed, and the three fields below will not be displayed.
Max user number 1	The FTP server can accommodate up to one user.
User count 0	The current login user number is 0.
Timeout value (in minute) 30	The connection idle time is 30 minutes.

Note

The 3com switch 4200G supports one user access at one time when it serves as the FTP server.

display ftp-server source-ip

Syntax

display ftp-server source-ip

View

Any view

Parameters

None

Description

Use the **display ftp-server source-ip** command to display the source IP address set for an FTP server.

- If a source interface is specified for the FTP server, the IP address of the source interface will be displayed and the FTP client can only use this address as the destination address to connect to the FTP server.
- If neither source interface nor source IP address is specified, 0.0.0.0 will be displayed. In this case, the FTP client can use any reachable IP address on the FTP server as the destination address to connect to the FTP server.

To set the source IP address for an FTP server, use the **ftp-server source-interface** or the **ftp-server source-ip** command.

Examples

Display the source IP address configured for the FTP server.

```
<Sysname> display ftp-server source-ip
The source IP you specified is 192.168.0.1
```

display ftp-user

Syntax

display ftp-user

View

Any view

Parameters

None

Description

Use the **display ftp-user** command to display the information of the FTP users that have logged in to the switch, including the user name, host IP address, port number, idle timeout time, and authorized directory.

 **Note**

For how to create an FTP user on an FTP server, refer to the *AAA* part of this manual.

Examples

Display the information of the FTP users that have logged in to the switch.

```
<Sysname> display ftp-user
  UserName             HostIP    Port    Idle             HomeDir
admin           192.168.0.152    1029       0              flash:
```

If the username exceeds ten characters, characters behind the tenth will be displayed in the second line with a left-aligning mode. Take username **username@test** for example, the result is:

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

Table 1-2 display ftp-user command output description

Field	Description
HostIP	IP address of the FTP client
Port	Port used when the FTP client logs in
Idle	Idle time of the FTP client
HomeDir	The initial work path configured for the FTP user, namely, the path where the user locates after he logs in.

ftp disconnect

Syntax

ftp disconnect *user-name*

View

System view

Parameters

user-name: Name of the user to be disconnected from the FTP server, a string of 1 to 184 characters.

Description

Use the **ftp disconnect** command to terminate the connection between a specified user and the FTP server.

Note

With a 3com switch 4200G acting as the FTP server, if you attempt to disconnect a user that is uploading/downloading data to/from the FTP server, the switch 4200G will disconnect the user after the data transmission is completed.

Related commands: **display ftp-user**.

Examples

Display the current online FTP users.

```
<Sysname> display ftp-user
  UserName             HostIP    Port    Idle              HomeDir
admin           192.168.0.152    1029       0               flash:
```

Disconnect the user named **admin** from the FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp disconnect admin
% The user connection will be disconnected after the data transfer finished
[Sysname]
%Apr  2 01:06:14:915 2000 Sysname FTPS/5/USEROUT:- 1 -User admin(192.168.0.152) logged out
```

ftp server enable

Syntax

ftp server enable

undo ftp server

View

System view

Parameters

None

Description

Use the **ftp server enable** command to enable the FTP server function of the switch.

Use the **undo ftp server** command to disable the FTP server function of the switch.

By default, the FTP server function is disabled on the 3com switch 4200G to avoid potential security risks.

Note

To protect unused sockets from being attacked by malicious users, the 3com switch 4200G provides the following functions:

- TCP 21 is enabled only when you start the FTP server.
- TCP 21 is disabled after you shut down the FTP server.

Related commands: **display ftp-server**.

Examples

Enable the FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp server enable
% Start FTP server
```

ftp timeout

Syntax

ftp timeout *minutes*

undo ftp timeout

View

System view

Parameters

minutes: Idle timeout time (in minutes), in the range 1 to 35791.

Description

Use the **ftp timeout** command to set the idle timeout time of an FTP client. When the idle time of the FTP client exceeds this timeout time, the FTP server terminates the connection with the FTP client.

Use the **undo ftp timeout** command to restore the default idle timeout time.

By default, the idle timeout time is 30 minutes.

If an FTP connection between an FTP server and an FTP client breaks down abnormally, but the FTP server cannot be aware of this, the FTP server will keep this connection. This will occupy system resources and affect other FTP users' log in. You can set an idle timeout time so that the FTP server considers an FTP connection invalid and terminates it if no data exchange occurs on it in idle timeout time.

Examples

Set the idle timeout time to 36 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp timeout 36
```

ftp-server source-interface

Syntax

ftp-server source-interface *interface-type interface-number*

undo ftp-server source-interface

View

System view

Parameters

interface-type: Type of the interface serving as the source interface of an FTP server. The interface type can be a loopback interface or a VLAN interface.

interface-number: Number of the source interface of an FTP server.

Description

Use the **ftp-server source-interface** command to specify the source interface for an FTP server. After you execute this command, users can only use the IP address of the specified source interface as the destination address to connect to an FTP server, which can enhance security of the FTP server.

Use the **undo ftp-server source-interface** command to cancel the source interface setting.

By default, no source interface is specified for an FTP server, and an FTP client can use any reachable interface address on the FTP server as the destination address to connect to the FTP server.

Related commands: **ftp-server source-ip**.

Examples

Specify VLAN-interface 1 as the source interface of the FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp-server source-interface Vlan-interface 1
```

ftp-server source-ip

Syntax

ftp-server source-ip *ip-address*

undo ftp-server source-ip

View

System view

Parameters

ip-address: The source IP address of an FTP server.

Description

Use the **ftp-server source-ip** command to specify the source IP address for an FTP server. After you execute this command, users can only use the specified source IP address as the destination address to connect to the FTP server. The value of argument *ip-address* must be an IP address on the device where the configuration is performed. Otherwise, a prompt appears to show the configuration fails.

Use the **undo ftp-server source-ip** command to cancel the source IP address setting. By default, no source IP address is specified for an FTP server, and an FTP client can use any reachable address on the FTP server as the destination address to connect to an FTP server.

Examples

Specify 192.168.1.1 as the source IP address of the FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp-server source-ip 192.168.1.1
```

FTP Client Configuration Commands

Note

- In the examples of this section, if a command should be executed in FTP client view, the configuration process for entering FTP client view will be omitted to avoid repetition. For the configuration of the command for entering FTP client view, refer to ftp.
- When executing the FTP client configuration commands in this section, confirm whether the corresponding access rights are configured on the FTP server, for example, query file lists under a working directory, read/download the specified files, create a directory/upload a file, and rename/delete a file on the server. For the configuration of user access rights, refer to the FTP server software description.

---

ascii

Syntax

ascii

View

FTP client view

Parameters

None

Description

Use the **ascii** command to specify that files be transferred in ASCII mode, which is used for transferring text files.

By default, files are transferred in ASCII mode.

Related commands: **binary**.

Examples

Specify to transfer text files in ASCII mode.

```
[ftp] ascii
```

```
200 Type set to A.
```

binary

Syntax

binary

View

FTP client view

Parameters

None

Description

Use the **binary** command to specify that program files be transferred in binary mode, which is used for transferring program files.

By default, files are transferred in ASCII mode.

Related commands: **ascii**.

Examples

Specify to transfer files in binary mode.

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

bye

Syntax

bye

View

FTP client view

Parameters

None

Description

Use the **bye** command to terminate the control connection and data connection with the FTP server and return to user view.

This command has the same effect as that of the **quit** command.

Examples

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

```
[ftp] bye
221 Server closing.
<Sysname>
```

cd

Syntax

cd *path*

View

FTP client view

Parameters

path: Path of the target directory.

Description

Use the **cd** command to change the working directory on the remote FTP server.

Note that you can use this command to enter only authorized directories.

Related commands: **pwd**.

Examples

Change the working directory to **flash:/temp**.

```
[ftp] cd flash:/temp
```

Display the current working directory.

```
[ftp] pwd
257 "flash:/temp" is current directory.
```

cdup

Syntax

cdup

View

FTP client view

Parameters

None

Description

Use the **cdup** command to exit the current working directory and enter the parent directory. The parent directory must be a directory that a user is authorized to access; otherwise, the command cannot be executed.

Related commands: **cd**, **pwd**.

Examples

Change the working directory to **flash:/temp**.

```
[ftp] cd flash:/temp
```

Change the working directory to the parent directory.

```
[ftp] cdup
```

Display the current directory.

```
[ftp] pwd
257 "flash:" is current directory.
```

close

Syntax

close

View

FTP client view

Parameters

None

Description

Use the **close** command to terminate an FTP connection without quitting FTP client view.

This command has the same effect as that of the **disconnect** command.

Examples

Terminate the FTP connection without quitting FTP client view.

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

delete

Syntax

delete *remotefile*

View

FTP client view

Parameters

remotefile: Name of the file to be deleted.

Description

Use the **delete** command to delete a specified remote file.

Examples

Delete the file **temp.c**.

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

dir

Syntax

dir [*filename* [*localfile*]]

View

FTP client view

Parameters

filename: Name of the file to be queried.

localfile: Name of the local file where the query result is to be saved.

Description

Use the **dir** command to query specified files on a remote FTP server, or to display file information in the current directory. The output information, which includes the name, size and creation time of files, will be saved in a local file.

If you do not specify the *filename* argument, the information about all the files in the current directory is displayed.

Caution

You can use the **dir** command to display the file-related information such as file size, creation date, and so on. To display only the names of all the files under the current directory, use the **ls** command.

Related commands: **pwd**.

Examples

Display the information about all the files in the current directory on the remote FTP server.

```
[ftp] dir
227 Entering Passive Mode (192,168,0,152,4,0).
125 ASCII mode data connection already open, transfer starting for *.
-rwxrwxrwx   1 noone    nogroup    377424 Apr 26 13:05 s3r01.btm
-rwxrwxrwx   1 noone    nogroup    377424 Oct 10  2006 s3r01_15.btm
-rwxrwxrwx   1 noone    nogroup      2833 May 11 17:58 config.cfg
-rwxrwxrwx   1 noone    nogroup    225295 Apr 26 12:21 default.diag
-rwxrwxrwx   1 noone    nogroup    377424 Apr 30 16:58 switch.btm
drwxrwxrwx   1 noone    nogroup         0 Apr 28 11:41 test
-rwxrwxrwx   1 noone    nogroup      2145 Apr 28 13:13 test.txt
-rwxrwxrwx   1 noone    nogroup        13 Apr 28 13:21 mytest.bak
-rwxrwxrwx   1 noone    nogroup         9 Apr 28 13:24 a.txt
-rwxrwxrwx   1 noone    nogroup       142 Sep 10  2006 myopenssh
-rwxrwxrwx   1 noone    nogroup   5292802 Apr 30 17:02 switch2.bin
-rwxrwxrwx   1 noone    nogroup        15 Apr 26 17:45 public
-rwxrwxrwx   1 noone    nogroup        15 Apr 26 17:56 temp.c
```

```
-rwxrwxrwx   1 noone    nogroup   5286666 Oct 18  2006 switch5.bin
-rwxrwxrwx   1 noone    nogroup       306 May 13 11:17 swithc001
226 Transfer complete.
FTP: 1025 byte(s) received in 0.019 second(s) 53.00K byte(s)/sec.
```

Display information about file **config.cfg** and save the information to file **temp1**.

```
[ftp] dir config.cfg temp1
227 Entering Passive Mode (192,168,0,152,4,3).
125 ASCII mode data connection already open, transfer starting for config.cfg.
.....226 Transfer complete.
FTP: 67 byte(s) received in 5.818 second(s) 11.00 byte(s)/sec.
```

disconnect

Syntax

disconnect

View

FTP client view

Parameters

None

Description

Use the **disconnect** command to terminate an FTP connection without quitting FTP client view.

This command has the same effect as that of the **close** command.

Examples

Terminate the FTP connection without quitting FTP client view.

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

display ftp source-ip

Syntax

display ftp source-ip

View

Any view

Parameters

None

Description

Use the **display ftp source-ip** command to display the source IP address that the current device serving as an FTP client uses every time it connects to an FTP server. If a source IP address is specified

for the FTP client, the configured source IP address will be displayed. If neither a source IP address nor source interface is specified for the FTP client, 0.0.0.0 will be displayed.

If no source IP address is specified for the FTP client, the switch searches the entry with the destination as the subnet where the FTP server resides, and uses the IP address of the outbound interface in the entry as the source IP address.

Examples

Display the source IP address that the FTP client uses every time it connects to an FTP server.

```
<Sysname> display ftp source-ip
The source IP you specified is 192.168.0.1
```

ftp

Syntax

ftp [**cluster** | *remote-server* [*port-number*]]

View

User view

Parameters

cluster: Connects to the configured FTP server of a cluster. For the configuration of the FTP server of a cluster, refer to the *Cluster* part of this manual.

remote-server: Host name or IP address of an FTP server, a string of 1 to 20 characters.

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

Description

Use the **ftp** command to establish a control connection with an FTP server. If you enter a correct username and password, you can enter FTP client view.

Examples

Connect to the FTP server whose IP address is 2.2.2.2.

```
<Sysname> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):admin
331 Password required for admin.
Password:
230 User logged in.
[ftp]
```

ftp { cluster | *remote-server* } source-interface

Syntax

ftp { **cluster** | *remote-server* } **source-interface** *interface-type interface-number*

View

User view

Parameters

cluster: Connects to the configured FTP server of a cluster. For the configuration of the FTP server of a cluster, refer to the *Cluster* part of this manual.

remote-server: Host name or IP address of an FTP server, a string of 1 to 20 characters.

interface-type: Type of the source interface, which can be VLAN interface or loopback interface.

interface-number: Number of the source interface.

Description

Use the **ftp** { **cluster** | *remote-server* } **source-interface** command to configure the source IP address that the switch uses when it connects to an FTP server. The command takes effect only for the current connection process, and it will fail if the specified interface does not exist.

To make the configuration take effect forever, you can use the **ftp source-interface** command.

Examples

Configure that the switch uses VLAN-interface 1 as the source interface to connect to the FTP server whose IP address is 192.168.8.8

```
<Sysname> ftp 192.168.8.8 source-interface Vlan-interface 1
```

ftp { cluster | remote-server } source-ip

Syntax

ftp { **cluster** | *remote-server* } **source-ip** *ip-address*

View

User view

Parameters

cluster: Connects to the configured FTP server of a cluster. For the configuration of the FTP server of a cluster, refer to the *Cluster* part of this manual.

remote-server: Host name or IP address of an FTP server, a string of 1 to 20 characters.

ip-address: Source IP address.

Description

Use the **ftp** { **cluster** | *remote-server* } **source-ip** command to configure the source IP address that the switch uses when it connects to an FTP server. The command takes effect only for the current connection, and it will fail if the specified source IP address does not exist.

To make the configuration take effect forever, you can use the **ftp source-ip** command.

Examples

Configure that the switch uses 192.168.0.1 as the source address to connect to the FTP server whose IP address is 192.168.8.8.

```
<Sysname> ftp 192.168.8.8 source-ip 192.168.0.1
```

ftp source-interface

Syntax

ftp source-interface *interface-type interface-number*

undo ftp source-interface

View

System view

Parameters

interface-type: Type of the source interface, which can be VLAN interface or loopback interface.

interface-number: Number of the source interface.

Description

Use the **ftp source-interface** command to specify a source interface as the source interface the switch uses every time it connects to an FTP server, and the configuration will be saved to the configuration file of the system.

Use the **undo ftp source-interface** command to cancel the source interface setting. After you execute this command, the FTP client system decides which interface will be used for accessing FTP servers.

By default, the switch uses the IP address of the outbound interface in the local routing table as the source IP address for connecting to an FTP server. The destination of the outbound interface is the subnet where the FTP server resides.

To configure the source interface used only for the current connection to an FTP server, use the **ftp** { **cluster** | *remote-server* } **source-interface** command.

Examples

Specify VLAN-interface 1 as the source interface to be used in each connection between the switch and an FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp source-interface Vlan-interface 1
```

ftp source-ip

Syntax

ftp source-ip *ip-address*

undo ftp source-ip

View

System view

Parameters

ip-address: IP address that is to be specified as the source IP address.

Description

Use the **ftp source-ip** command to specify the source IP address of that the switch uses every time it connects to an FTP server, and the configuration will be saved to the configuration file of the system. The value of argument *ip-address* must be an IP address on the device where the configuration is performed. Otherwise, a prompt appears to show the configuration fails.

Use the **undo ftp source-ip** command to cancel the source IP address setting.

By default, the switch uses the IP address of the outbound interface in the local routing table as the source IP address for connecting to an FTP server. The destination of the outbound interface is the subnet where the FTP server resides.

Examples

Specify 192.168.0.1 as the source IP address that the switch uses every time it connects to an FTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ftp source-ip 192.168.0.1
```

get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

Parameters

remotefile: Name of a file to be downloaded.

localfile: File name used when a file is downloaded and saved to the local device. If this argument is not specified, the source file name is used when a file is saved and downloaded to the local device.

Description

Use the **get** command to download a remote file and save it as a local file.

Caution

When using the **get** command to download files from a remote FTP server, note to limit the length of file path and file name within the following ranges:

- A directory name should be no more than 91 characters.
- A file name plus its local path name should be no more than 127 characters.
- A device name should be no more than 14 characters.
- A file name plus its complete path name should be no more than 142 characters.

Examples

Download file **temp.c**.

```
[ftp] get temp.c
227 Entering Passive Mode (2,2,2,2,4,12).
125 ASCII mode data connection already open, transfer starting for temp.c.
..226 Transfer complete.
FTP: 15 byte(s) received in 2.568 second(s) 0.00 byte(s)/sec.
```

lcd

Syntax

lcd

View

FTP client view

Parameters

None

Description

Use the **lcd** command to display the local working directory on the FTP client. If you have logged in to the FTP server, you cannot modify the local working directory of the FTP client; to modify the local working directory, you need to terminate the connection with the FTP server, quit FTP client view, execute the **cd** command in user view, and reconnect to the FTP server.

Examples

Display the local working directory on the FTP client.

```
[ftp] lcd
% Local directory now flash:/temp
```

ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

Parameters

remotefile: Name of the file to be queried.

localfile: Name of the local file where the querying result is to be saved.

Description

Use the **ls** command to display the information about a specified file on an FTP server.

If you do not specify the *remotefile* argument, names of all the files in the current remote directory are displayed.

Caution

The **ls** command only displays file names on an FTP server. To query other file-related information, for example, file size, creation date and so on, use the **dir** command.

Related commands: **pwd**.

Examples

Display the names of all the files in the current directory on the remote FTP server.

```
[ftp] ls
227 Entering Passive Mode (2,2,2,2,4,4).
125 ASCII mode data connection already open, transfer starting for *.
s3r01.btm
s3r01_15.btm
config.cfg
default.diag
test
test.txt
mytest.bak
a.txt
myopenssh
public
temp.c
swithc001
226 Transfer complete.
FTP: 200 byte(s) received in 0.145 second(s) 1.00Kbyte(s)/sec.
```

mkdir

Syntax

mkdir *pathname*

View

FTP client view

Parameters

pathname: Name of the directory to be created.

Description

Use the **mkdir** command to create a directory on an FTP server.

Related commands: **dir**, **rmdir**.

Examples

Create the directory **flash:/lanswitch** on the FTP server.

```
[ftp] mkdir flash:/lanswitch
257 "flash:/ lanswitch" new directory created.
```

open

Syntax

open { *ip-address* | *server-name* } [*port*]

View

FTP client view

Parameters

ip-address: IP address of an FTP server.

server-name: Host name of the FTP server, a string of 1 to 20 characters.

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

Description

Use the **open** command to establish a control connection with an FTP server. If you have connected to an FTP server, you cannot use the **open** command to connect to another server, and you need to terminate the connection with the current FTP server and then execute the **open** command.

Related commands: **close**.

Examples

Establish a control connection with the FTP server whose IP address is 1.1.1.1 in FTP client view.

```
[ftp]open 1.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):abc
331 Password required for abc
Password:
230 User logged in.
```

passive

Syntax

passive

undo passive

View

FTP client view

Parameters

None

Description

Use the **passive** command to set the data transfer mode to the passive mode.

Use the **undo passive** command to set the data transfer mode to the active mode.

By default, the passive mode is adopted.

The differences between the passive mode and the active mode are:

- When working in the active mode, an FTP client advertises a random port Port1 to an FTP server through TCP port 21; upon receiving the advertisement, the FTP server initiates a connection with Port1 on the client for data transmission.
- When working in the passive mode, an FTP client sends a passive request to the FTP server before data transmission, the FTP server advertises a local random port Port2 to the FTP client, and the FTP client establishes a connection with Port2 using a local random port.

If an FTP client initiates a connection with an FTP server through a firewall, the firewall may block the connection request because the FTP server initiates the connection with Port1 through an external network, and thus data transmission will be affected. Therefore, you are recommended to set the data transmission mode of the FTP client to passive when accessing the FTP server through a firewall.

Examples

Set the data transfer mode to the passive mode.

```
[ftp] passive
% Passive is on
```

put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

Parameters

localfile: Name of a local file to be uploaded.

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

Description

Use the **put** command to upload a local file on an FTP client to an FTP server.

If you do not specify the *remotefile* argument, the local file is saved on the FTP server with its original name.

Examples

Upload the local file named **temp.c** to the FTP server.

```
[ftp] put temp.c
227 Entering Passive Mode (2,2,2,2,4,13).
125 ASCII mode data connection already open, transfer starting for temp.c.
226 Transfer complete.
FTP: 15 byte(s) sent in 7.549 second(s) 1.00byte(s)/sec.
```

pwd

Syntax

pwd

View

FTP client view

Parameters

None

Description

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

Related commands: **cd**, **cdup**, **dir**, **ls**.

Examples

Display the working directory on the FTP server.

```
[ftp] pwd
257 "flash:/temp" is current directory.
```

quit

Syntax

quit

View

FTP client view

Parameters

None

Description

Use the **quit** command to terminate FTP control connection and FTP data connection and return to user view.

This command has the same effect as that of the **bye** command.

Examples

Terminate the FTP control connection and FTP data connection and return to user view.

```
[ftp] quit
221 Server closing.
<Sysname>
```

remotehelp

Syntax

remotehelp [*protocol-command*]

View

FTP client view

Parameters

protocol-command: FTP protocol command.

Description

Use the **remotehelp** command to display the help information about an FTP protocol command.

This command works only when the FTP server provides the help information about FTP protocol commands.

Caution

- This command is always valid when a 3com switch operates as the FTP server.
- If you use other FTP server software, refer to related instructions to know whether the FTP server provides help information about FTP protocol commands.

Examples

Display the syntax of the **user** command.

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

rename

Syntax

rename *remote-source remote-dest*

View

FTP client view

Parameters

remote-source: Name of a file on a remote host.

remote-dest: Destination file name.

Description

Use the **rename** command to rename a file on a remote FTP server.

If the destination file name conflicts with the name of an existing file or directory, you will fail to rename the file.

Examples

Rename file **temp.c** as **forever.c**.

```
[ftp] rename temp.c forever.c
350 Enter the name to rename it to...
```

```
250 File renamed successfully
```

rmdir

Syntax

rmdir *pathname*

View

FTP client view

Parameters

pathname: Name of a directory on an FTP server.

Description

Use the **rmdir** command to remove a specified directory on an FTP server.

Note that you can only use this command to remove directories that are empty.

Examples

Remove the directory **flash:/temp1** on the FTP server. (Assume that the directory is empty.)

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

user

Syntax

user *username* [*password*]

View

FTP client view

Parameters

username: Username used to log in to an FTP server.

password: Password used to log in to an FTP server.

Description

Use the **user** command to log in to an FTP server with the specified username and password.

Examples

Log in to the FTP server using the user account with the username **tom** and the password **111**.

```
[ftp] user tom 111
331 Password required for tom.
230 User logged in.verbose
```

verbose

Syntax

verbose

undo verbose

View

FTP client view

Parameters

None

Description

Use the **verbose** command to enable the verbose function, which displays execution information of user operations and all FTP responses.

Use the **undo verbose** command to disable the verbose function.

The verbose function is enabled by default.

Examples

Download the file with name **test1.cfg**.

```
[ftp] get test1.cfg

227 Entering Passive Mode (192,168,0,3,5,239)
150 "D:\FTP\test1.cfg" file ready to send (100 bytes) in ASCII mode
....226 Transfer finished successfully.
FTP: 100 byte(s) received in 5.109 second(s) 20.00 byte(s)/sec.
```

Disable the verbose function.

```
[ftp] undo verbose
```

Download the file with name **test.cfg**.

```
[ftp] get test.cfg
......FTP: 1740 byte(s) received in 9.367 second(s) 185.00 byte(s)/sec.
```

The above output indicates that if the verbose function is disabled, only execution information of users' operations is obtained from the system of the switch, while the output information beginning with three-digit numbers cannot be returned to the users.

For the description of the numbers at the beginning of FTP output information, refer to the corresponding section in RFC 959.

SFTP Server Configuration Commands

sftp server enable

Syntax

sftp server enable

undo sftp server

View

System view

Parameters

None

Description

Use the **sftp server enable** command to enable the SFTP server.

Use the **undo sftp server** command to disable the SFTP server.

By default, the SFTP server is disabled.

Examples

Enable the SFTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sftp server enable
%Start SFTP server
```

sftp timeout

Syntax

sftp timeout *time-out-value*

undo sftp timeout

View

System view

Parameters

time-out-value: Timeout time, in the range 1 to 35,791, in minutes. The default value is 10.

Description

Use the **sftp timeout** command to set the idle timeout time on an SFTP server.

Use the **undo sftp timeout** command to restore the idle timeout time to the default value.

If the idle timeout time exceeds the specified threshold, the system disconnects the SFTP user automatically.

Examples

Set the idle timeout time to 500 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sftp timeout 500
```

SFTP Client Configuration Commands

bye

Syntax

bye

View

SFTP client view

Parameters

None

Description

Use the **bye** command to terminate a connection with the remote SFTP server and return to system view.

This command has the same effect as that of the commands **exit** and **quit**.

Examples

Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
[Sysname]
```

cd

Syntax

cd [*remote-path*]

View

SFTP client view

Parameters

remote-path: Path of the target directory on the remote server.

Description

Use the **cd** command to change the working path on the remote SFTP server. If no remote path is specified, this command displays the current working path.

Note

- Use the **cd ..** command to return to the parent directory.
- Use the **cd /** command to return to the root directory.

Examples

Change the working path to new1.

```
sftp-client>cd new1
Received status: Success
Current Directory is:
/new1
sftp-client>
```

cdup

Syntax

cdup

View

SFTP client view

Parameters

None

Description

Use the **cdup** command to change the working path on the remote SFTP server and return to the parent directory.

Examples

Change the working path and return to the parent directory.

```
sftp-client>cdup
Received status: Success
Current Directory is:
/
```

delete

Syntax

delete *remote-file*&<1-10>

View

SFTP client view

Parameters

remote-file&<1-10>: Name of a file on the server. &<1-10> indicates that up to ten file names can be input. These file names should be separated by spaces.

Description

Use the **delete** command to delete a specified file from the remote SFTP server.

This command has the same effect as that of the **remove** command.

Examples

Delete the file named test.txt on the server.

```
sftp-client> delete test.txt
The following files will be deleted:
/test.txt
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
```

dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Parameters

-a: Displays the file and folder names in a specified directory.

-l: Displays the details about files and folders in a specified directory in a list.

remote-path: Name of the path where the file and folders to be queried reside.

Description

Use the **dir** command to query a specified directory on the remote SFTP server.

If **-a** or **-l** is not specified, the command displays details about the files and folders in the specified directory in a list.

If no remote path is specified, this command displays the files in the current working directory.

This command has the same effect as that of the **ls** command.

Examples

Display the files in the current directory.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
Received status: End of file
Received status: Success
```

display sftp source-ip

Syntax

display sftp source-ip

View

Any view

Parameters

None

Description

Use the **display sftp source-ip** command to display the source IP address specified for the current SFTP client.

If you have specified a source interface for the SFTP client, this command displays the IP address of the source interface; otherwise, this command displays the IP address 0.0.0.0.

Examples

Display the source IP address for the current SFTP client.

```
<Sysname> display sftp source-ip
The source IP you specified is 192.168.1.1
```

exit

Syntax

exit

View

SFTP client view

Parameters

None

Description

Use the **exit** command to terminate a connection with the remote SFTP server and return to system view.

This command has the same effect as that of the commands **bye** and **quit**.

Examples

Terminate a connection with the remote SFTP server.

```
sftp-client> exit
Bye
[Sysname]
```

get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

Parameters

remote-file: Name of a file on the remote SFTP server.

local-file: Name of a local file.

Description

Use the **get** command to download a file from the remote server.

By default, the remote file name is used for the file saved locally if no local file name is specified.

Examples

Download the file **tt.bak** and save it with the name **tt.txt**.

```
sftp-client>get tt.bak tt.txt....
This operation may take a long time, please wait...
Remote  file:tt.bak --->  Local file: tt.txt..
Received status: End of file
Received status: Success
Downloading file successfully ended
```

help

Syntax

help [**all** |*command*]

View

SFTP client view

Parameters

all: Displays all the command names.

command: Command name.

Description

Use the **help** command to display the help information about SFTP client commands.

If no command is specified, this command displays all the command names.

Examples

View the help information about the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file.Default local-path is the same
                              with remote-path
```

ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Parameters

-a: Displays the file and folder names in a specified directory.

-l: Displays the details about files and folders in a specified directory in a list.

remote-path: Name of the path where the files and folders to be queried reside.

Description

Use the **ls** command to display files in a specified directory on the remote SFTP server.

If **-a** or **-l** is not specified, the command displays details about the files and folders in the specified directory in a list.

If no remote path is specified, this command displays the files in the current working directory.

This command has the same effect as that of the **dir** command.

Examples

Display the files in the current 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
Received status: End of file
Received status: Success
```

mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

Parameters

remote-path: Name of a directory on the remote SFTP server.

Description

Use the **mkdir** command to create a directory on the remote SFTP server.

Examples

Create a directory named **hj** on the remote SFTP server.

```
sftp-client>mkdir hj
Received status: Success
New directory created
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

Parameters

local-file: Name of a local file.

remote-file: Name of a file on the remote SFTP server.

Description

Use the **put** command to upload a local file to the remote SFTP server.

By default, the local file name is used for the remote file if no remote file name is specified.

Examples

Upload the file named config.cfg to the remote SFTP server and save it as 1.txt.

```
sftp-client>put config.cfg 1.txt
This operation may take a long time, please wait...
Local file:config.cfg --->  Remote file: /1.txt
Received status: Success
Uploading file successfully ended
```

pwd

Syntax

pwd

View

SFTP client view

Parameters

None

Description

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

Examples

Display the working directory on the remote SFTP server.

```
sftp-client> pwd
/
```

quit

Syntax

quit

View

SFTP client view

Parameters

None

Description

Use the **quit** command to terminate a connection with the remote SFTP server and return to system view.

This command has the same effect as that of the commands **bye** and **exit**.

Examples

Terminate a connection with the remote SFTP server.

```
sftp-client> quit
Bye
[Sysname]
```

remove

Syntax

remove *remote-file*&<1-10>

View

SFTP client view

Parameters

remote-file&<1-10>: Name of a file on the server. &<1-10> indicates that up to ten file names can be input. These file names should be separated by spaces.

Description

Use the **remove** command to delete a specified file from the remote SFTP server.

This command has the same effect as that of the **delete** command.

Examples

Delete the file named temp.c from the server.

```
sftp-client> remove temp.c
The followed File will be deleted:
/temp.c
Are you sure to delete it?(Y/N):y
```

```
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
```

rename

Syntax

rename *oldname newname*

View

SFTP client view

Parameters

oldname: Old file name.

newname: New file name.

Description

Use the **rename** command to rename a specified file on the remote SFTP server.

Examples

Change the file name **temp.bat** to **temp.txt**.

```
sftp-client> rename temp.bat temp.txt
File successfully renamed
```

rmdir

Syntax

rmdir *remote-path*&<1-10>

View

SFTP client view

Parameters

remote-path&<1-10>: Name of a directory on the remote SFTP server. &<1-10> indicates that up to ten file names can be input. These file names should be separated by spaces.

Description

Use the **rmdir** command to remove a specified directory from the remote SFTP server.

Examples

Remove the directory **hello** on the SFTP server.

```
sftp-client>rmdir hello
The followed directory will be deleted
/hello
Are you sure to remove it?(Y/N):y
This operation may take a long time.Please wait...
```

```
Received status: Success
Directory successfully removed
```

sftp

Syntax

sftp { *host-ip* | *host-name* } [*port-num*] [**identity-key** { **dsa** | **rsa** } | **prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **3des** | **des** | **aes128** } | **prefer_stoc_cipher** { **3des** | **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *

View

System view

Parameters

host-ip: IP address of the server.

host-name: Host name of the server, a string of 1 to 20 characters.

port-num: Port number of the server, in the range of 0 to 65535. The default value is 22.

identity-key: The public key algorithm used by the publickey authentication. **rsa** is the default.

- **dsa**: The public key algorithm is DSA.
- **rsa**: The public key algorithm is RSA.

prefer_kex: Specifies a preferred key exchange algorithm. You can select either of the two algorithms.

- **dh_group1**: Key exchange algorithm diffie-hellman-group1-sha1. It is the default key exchange algorithm.
- **dh_exchange_group**: Key exchange algorithm diffie-hellman-group-exchange-sha1.

prefer_ctos_cipher: Preferred client-to-server encryption algorithm. The default algorithm is aes128.

prefer_stoc_cipher: Preferred server-to-client encryption algorithm. The default algorithm is aes128.

- **3des**: 3des_cbc encryption algorithm. Support for this keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not.
- **des**: des_cbc encryption algorithm.
- **aes128**: aes_128 encryption algorithm.

prefer_ctos_hmac: Preferred client-to-server HMAC algorithm. The default algorithm is sha1_96.

prefer_stoc_hmac: Preferred server-to-client HMAC algorithm. The default algorithm is sha1_96.

- **sha1**: HMAC algorithm hmac-sha1.
- **sha1_96**: HMAC algorithm hmac-sha1-96.
- **md5**: HMAC algorithm hmac-md5.
- **md5_96**: HMAC algorithm hmac-md5-96.

Description

Use the **sftp** command to establish a connection with the remote SFTP server and enter SFTP client view.

If you specify to authenticate a client through public key on the server, the client needs to read the local private key when logging in to the SFTP server. Since both RSA and DSA are available for public key authentication, you need to use the **identity-key** key word to specify the algorithms to get correct local private key; otherwise you will fail to log in.

Examples

Connect the SFTP server with the IP address 10.1.1.2. Use the default encryption algorithm.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]sftp 10.1.1.2
Input Username: kk
Trying 10.1.1.2...
Press CTRL+K to abort
Connected to 10.1.1.2 ...

The Server is not authenticated. Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
Enter password:

sftp-client>
```

sftp source-interface

Syntax

sftp source-interface *interface-type interface-number*

undo sftp source-interface

View

System view

Parameters

interface-type: Type of a source interface. It can be loopback or VLAN interface.

interface-number: Number of a source interface.

Description

Use the **sftp source-interface** command to specify a source interface for the SFTP client. If the specified interface does not exist, the system prompts that the configuration fails.

Use the **undo sftp source-interface** command to remove the specified source interface. Then the client accesses the SFTP server with the local device address determined by the system.

Examples

Specify VLAN-interface 1 as the source interface of the SFTP client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sftp source-interface Vlan-interface 1
```

sftp source-ip

Syntax

sftp source-ip *ip-address*

undo sftp source-ip

View

System view

Parameters

ip-address: Source IP address to be set.

Description

Use the **sftp source-ip** command to specify a source IP address for the SFTP client. If the specified IP address is not the IP address of the local device, the system prompts that the configuration fails.

Use the **undo sftp source-ip** command to remove the specified source IP address. Then the client accesses the SFTP server with the local device address determined by the system.

Examples

Specify 192.168.0.1 as the source IP address of the SFTP client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sftp source-ip 192.168.0.1
```

2 TFTP Configuration Commands

TFTP Configuration Commands

Note

When accessing a TFTP server configured with an IPv6 address, use the **tftp ipv6** command. For details, refer to the *IPv6 Management* part in this manual.

display tftp source-ip

Syntax

display tftp source-ip

View

Any view

Parameters

None

Description

Use the **display tftp source-ip** command to display the source IP address that a TFTP client uses every time it connects to a TFTP server (use the **tftp source-ip** command). If a source interface is specified for the TFTP client with the **tftp source-interface** command, the IP address of the source interface is displayed. If neither source IP address nor source interface is specified for the TFTP client, 0.0.0.0 is displayed.

Related commands: **tftp source-ip**, **tftp-source-interface**.

Examples

Display the source IP address that a TFTP client uses every time it connects to a TFTP server.

```
<Sysname> display tftp source-ip
The source IP you specified is 192.168.0.1
```

tftp { ascii | binary }

Syntax

tftp { **ascii** | **binary** }

View

System view

Parameters

ascii: Transfers data in ASCII mode, which is used for transferring text files.

binary: Transfers data in binary mode, which is used for transferring program files.

Description

Use the **tftp** { **ascii** | **binary** } command to set the TFTP data transfer mode.

By default, the binary mode is adopted.

Examples

Specify to adopt the ASCII mode.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tftp ascii
TFTP transfer mode changed to ASCII.
```

tftp get

Syntax

tftp *tftp-server* **get** *source-file* [*dest-file*]

View

User view

Parameters

tftp-server: IP address or the host name of a TFTP server, a string of 1 to 20 characters. If the switch belongs to a cluster, the value cluster means to connect to the TFTP server of the cluster. For the configuration of the TFTP server of a cluster, refer to the *Cluster* part in this manual.

source-file: Name of the file to be downloaded from the TFTP server.

dest-file: File name used when a file is downloaded and saved to the switch.

Description

Use the **tftp get** command to download a file from a TFTP server, and save it to the local storage device.

Different from the FTP function, the working directory of a TFTP server cannot be changed or specified on a TFTP client. To enter another working directory, you need to modify the working directory on the TFTP server and relog in.

The 3com switch 4200G supports the TFTP file size negotiation function, namely, before downloading a file, the switch requests the size of the file to be downloaded to the TFTP server, thus to ensure whether there is enough space on the Flash for file downloading. If the TFTP server also supports the function, when the file size is too large, the switch can know this in advance and stops the download operation to save network resources; if the TFTP server does not support the function, the switch can only download the file to its memory, and delete the file if it finds the file is too large when writing the file to the Flash.

Related commands: **tftp put**.

Examples

Download file **abc.txt** from the TFTP server whose IP address is 1.1.1.1 and save it as **efg.txt** (suppose free space of the flash memory is sufficient).

```
<Sysname> tftp 1.1.1.1 get abc.txt efg.txt
  File will be transferred in binary mode.
  Downloading file from remote tftp server, please wait......
  TFTP:       35 bytes received in 0 second(s).
  File downloaded successfully.
```

Download file **temp.txt** from the TFTP server (1.1.1.1) and save it as **test1.txt** (suppose that free space of the Flash is insufficient and the TFTP server does not support file size negotiation).

```
<Sysname> tftp 1.1.1.1 get temp.txt test1.txt
  File will be transferred in binary mode.
  Downloading file from remote tftp server, please wait......
  Not enough space; Writing to device failed; Downloaded data will be deleted.............
  Deleting file successful.
```

Download file **temp.txt** from the TFTP server (1.1.1.1) and save it as **test2.txt** (suppose that free space of the Flash is insufficient and the TFTP server supports file size negotiation).

```
<Sysname> tftp 1.1.1.1 get temp.txt test2.txt
  File will be transferred in binary mode.
  Downloading file from remote tftp server, please wait......
  Not enough space; Quit writing to device; Created file will be deleted...
  Deleting file successful.
```

tftp put

Syntax

tftp *tftp-server* **put** *source-file* [*dest-file*]

View

User view

Parameters

tftp-server: IP address or the host name of a TFTP server, a string of 1 to 20 characters. If the switch belongs to a cluster, the value cluster means to connect to the TFTP server of the cluster. For the configuration of the TFTP server of a cluster, refer to the *Cluster* part in this manual.

source-file: Name of the file to be uploaded to the TFTP server.

dest-file: File name used when a file is uploaded and saved to a TFTP server.

Description

Use the **tftp put** command to upload a file to a specified directory on a TFTP server.

When uploading files to a TFTP server, you can only select the files under the current working directory of the device. To upload files in another directory, use the **cd** command to change to the specified directory in user view before executing the **tftp put** command. For the execution of the **cd** command, refer to the *File System Management* part in this manual.

Related commands: **tftp get**.

Examples

Upload file **config.cfg** to the TFTP server whose IP address is 1.1.1.1 and save it as **temp.cfg**.

```
<Sysname> tftp 1.1.1.1 put config.cfg temp.cfg
  File will be transferred in binary mode.
  Copying file to remote tftp server. Please wait... /
  TFTP:      962 bytes sent in 0 second(s).
  File uploaded successfully.
```

tftp *tftp-server* source-interface

Syntax

tftp *tftp-server* **source-interface** *interface-type interface-number* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }

View

User view

Parameters

tftp-server: IP address or host name of the TFTP server to be connected to, a string of 1 to 20 characters. If the switch belongs to a cluster, the value cluster means to connect to the TFTP server of the cluster. For the configuration of the TFTP server of a cluster, refer to the *Cluster* part in this manual.

interface-type: Type of the source interface.

interface-number: Number of the source interface.

get: Specifies to download a file from the TFTP server.

source-file: Name of the file to be downloaded.

dest-file: File name used when a file is downloaded and saved to the switch.

put: Specifies to upload a file to the TFTP server.

source-file-url: Path and name of the file to be uploaded to the TFTP server.

dest-file: File name used when a file is uploaded and saved to a TFTP server.

Description

Use the **tftp** *tftp-server* **source-interface** command to connect to a TFTP server through the specified source interface, and perform download or upload operations. If the specified source interface does not exist, a prompt appears to show the command fails to be executed.

Examples

Connect to the remote TFTP server whose IP address is 192.168.8.8 through the source interface VLAN-interface 1, and download the file named **test.bin** from it.

```
<Sysname> tftp 192.168.8.8 source-interface Vlan-interface 1 get test.bin
```

tftp *tftp-server* source-ip

Syntax

tftp *tftp-server* **source-ip** *ip-address* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }

View

User view

Parameters

tftp-server: IP address or host name of the TFTP server to be connected to, a string of 1 to 20 characters. If the switch belongs to a cluster, the value cluster means to connect to the TFTP server of the cluster. For the configuration of the TFTP server of a cluster, refer to the *Cluster* part in this manual.

ip-address: IP address to be set as the source IP address.

get: Specifies to download a file from the TFTP server.

source-file: Name of the file to be downloaded.

dest-file: File name used when a file is downloaded and saved to the switch.

put: Specifies to upload a file to the TFTP server.

source-file-url: Path and name of the file to be uploaded to the TFTP server.

dest-file: File name used when a file is uploaded and saved to a TFTP server.

Description

Use the **tftp** *tftp-server* **source-ip** command to connect to a TFTP server through the specified source IP address, and perform download or upload operations. If the specified source IP address does not exist, a prompt appears to show the command fails to be executed.

Examples

Connect to the remote TFTP server whose IP address is 192.168.8.8 through the source IP address 192.168.0.1, and download the file named **test.bin** from it.

```
<Sysname> tftp 192.168.8.8 source-ip 192.168.0.1 get test.bin
```

tftp source-interface

Syntax

tftp source-interface *interface-type interface-number*

undo tftp source-interface

View

System view

Parameters

interface-type interface-number: Source interface that the switch uses every time it connects to the TFTP server.

Description

Use the **tftp source-interface** command to specify the source interface of a TFTP client that the TFTP client uses every time it connects to a TFTP server. The system prompts that the configuration fails if the specified interface does not exist.

Use the **undo tftp source-interface** command to cancel the source interface setting. The switch uses the IP address of the outbound interface in the local routing table as the source IP address to connect to a TFTP server. The destination of the outbound interface is the subnet where the TFTP server resides

By default, no source interface is specified for the switch to connect to the TFTP server.

Examples

Specify VLAN-interface 1 as the source interface that the TFTP client uses every time it connects to a TFTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tftp source-interface Vlan-interface 1
```

tftp source-ip

Syntax

tftp source-ip *ip-address*

undo tftp source-ip

View

System view

Parameters

ip-address: The source IP address that the switch uses every time it connects to a TFTP server.

Description

Use the **tftp source-ip** command to specify the source IP address that a TFTP client uses every time it connects with a TFTP server. The specified IP address must exist; otherwise, a prompt appears to show the configuration fails.

Use the **undo tftp source-ip** command to cancel the source IP address setting. The switch uses the IP address of the outbound interface in the local routing table as the source IP address to connect to a TFTP server. The destination of the outbound interface is the subnet where the TFTP server resides.

By default, no source IP address is specified for the switch to connect to the TFTP server.

Examples

Specify 192.168.0.1 as the source IP address that the TFTP client uses every time it connects to a TFTP server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tftp source-ip 192.168.0.1
```

tftp-server acl

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

View

System view

Parameters

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

Description

Use the **tftp-server acl** command to specify the ACL adopted for the connection between a TFTP client and a TFTP server.

Use the **undo tftp-server acl** command to cancel all ACLs adopted.

Examples

Specify to adopt ACL 2000 on the TFTP client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tftp-server acl 2000
```

Table of Contents

1 Information Center Configuration Commands

Information Center Configuration Commands

display channel

Syntax

display channel [*channel-number* | *channel-name*]

View

Any view

Parameters

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description

Use the **display channel** command to display the settings of an information channel.

If no argument is specified in the command, the settings of all channels are displayed.

Examples

Display the settings of information 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      warning       Y      debugging     Y      debugging
```

display info-center

Syntax

display info-center [**unit** *unit-id*]

View

Any view

Parameters

unit-id: Unit ID of the device, the value is 1.

Description

Use the **display info-center** command to display the operation status of information center, the configuration of information channels, the format of time stamp.

Related commands: **info-center enable**, **info-center loghost**, **info-center logbuffer**, **info-center console channel, info-center monitor channel**, **info-center trapbuffer**, **info-center snmp channel**, **info-center timestamp**

Examples

Display the operation status of information center, the configuration of information channels, the format of time stamp of the current system.

```
<Sysname> display info-center
Information Center: enabled
Log host:
         the interface name of the source address : Vlan-interface1
         192.168.0.2, channel number : 2, channel name : loghost
         language : english, host facility local : 7
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, channel number : 4, channel name : logbuffer
         dropped messages : 0, overwritten messages : 586
Trap buffer:
         enabled,max buffer size : 1024, current buffer size : 256,
         current messages : 5, channel number : 3, channel name : trapbuffer
         dropped messages : 0, overwritten messages : 0
Information timestamp setting:
         log - date, trap - date, debug - boot
```

Table 1-1 Description on the fields of the **display info-center** command

Field	Description
Information Center	Status of the information center: enabled/disabled
Log host	Information about the log host, including its IP address, name and number of information channel, language and level of the log host
Console	Information about the console port, including name and number of its information channel
Monitor	Information about the monitor port, including name and number of its information channel
SNMP Agent	Information about SNMP Agent, including name and number of its information channel
Log buffer	Information about the log buffer, including its state (enabled or disabled), its maximum size, current size, current messages, information channel name and number, number of dropped messages, and number of overwritten messages

Field	Description
Trap buffer	Information about the trap buffer, including its state (enabled or disabled), maximum size, current size, current messages, channel number and name, number of dropped messages, and number of overwritten messages
Information timestamp setting:	Information about the time stamp setting, showing the time stamp format of the log, trap and debugging information

display logbuffer

Syntax

display logbuffer [**unit** *unit-id*] [**level** *severity* | **size** *buffersize*]* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Parameters

unit-id: Unit ID of the device, the value is 1.

level *severity*: Specifies an information severity level. For the value of *severity*, refer to Table 1-2.

Table 1-2 Severity level defined in the information center

Severity	Severity value	Description
emergencies	1	The system is unavailable.
alerts	2	Information that demands prompt reaction
critical	3	Critical information
errors	4	Error information
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed
informational	7	Informational information to be recorded
debugging	8	Information generated during debugging

size *buffersize*: Specifies the size of the log buffer (number of messages the log buffer holds) you want to display. The *buffersize* argument ranges from 1 to 1,024 and defaults to 512.

|: Filters output log information with a regular expression. For detailed information about regular expressions, refer to *Configuration File Management Command* in this manual.

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

exclude: Displays the log information excluding the specified characters.

include: Displays the log information including the specified characters.

regular-expression: Regular expression.

Description

Use the **display logbuffer** command to display the status of the log buffer and the records in the log buffer.

Examples

Display the status of the log buffer and the records in 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 : 91
```

The rest is omitted here.

Table 1-3 display logbuffer command output description

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the log buffer, defaults to 4.
Channel name	The channel name of the log buffer, defaults to logbuffer.
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

display logbuffer summary

Syntax

display logbuffer summary [**level** *severity*]

View

Any view

Parameters

Level *severity*: Specifies an information severity level. For the value of *severity*, refer to Table 1-2.

Description

Use the **display logbuffer summary** command to display the statistics of the log buffer.

Examples

Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
 EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     0     0     0     0    94     0     1     0
```

The above information indicates that there are 94 warnings and one **informational** information in the log buffer.

display trapbuffer

Syntax

display trapbuffer [**unit** *unit-id*] [**size** *buffersize*]

View

Any view

Parameters

unit-id: Unit ID of the device, the value is 1.

size *buffersize*: Specifies the size of the trap buffer (number of messages the buffer holds) you want to display. The *buffersize* argument ranges from 1 to 1,024 and defaults to 256.

Description

Use the **display trapbuffer** command to display the status of the trap buffer and the records in the trap buffer.

Absence of the **size** *buffersize* argument indicates that all trap information is displayed.

Examples

Display the status of the trap buffer and the records in the trap buffer.

```
<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 : 19

#Apr  1 23:55:35:859 2006 Sysname L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.4(linkUp): portIndex is 4227762, ifAdminStatus is 1, ifOperStatus
is 1

#Apr  1 23:55:36:059 2006 Sysname L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.4(linkUp): portIndex is 4227794, ifAdminStatus is 1, ifOperStatus
is 1
……
<Omitted>
```

info-center channel name

Syntax

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View

System view

Parameters

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, up to 30 characters in length. The name must start with an English letter, containing no special character but numbers and English letters only.

Description

Use the **info-center channel name** command to name the channel whose number is *channel-number* as *channel-name*.

Use the **undo info-center channel** command to restore the default name of the channel whose number is *channel-number*.

By default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Do not configure two different channels with the same name.

Examples

Name channel 0 as “execconsole”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center channel 0 name execconsole
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Parameters

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description

Use the **info-center console channel** command to set the channel through which information is output to the console.

Use the **undo info-center console channel** command to restore the default channel through which system information is output to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

This command works only when the information center is enabled.

Related commands: **info-center enable** and **display info-center**.

Examples

Configure to output information to the console through channel 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center console channel 0
```

info-center enable

Syntax

info-center enable

undo info-center enable

View

System view

Parameters

None

Description

Use the **info-center enable** command to enable the information center.

Use the **undo info-center enable** command to disable the information center.

The switch can output system information to the log host, the console, and other destinations only when the information center is enabled.

By default, the information center is enabled.

Related commands: **display info-center**, **info-center loghost**, **info-center logbuffer**, **info-center console channel**, **info-center monitor channel**, **info-center trapbuffer**, **info-center snmp channel**.

Examples

Enable the information center.

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

info-center logbuffer

Syntax

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*

undo info-center logbuffer [**channel** | **size**]

View

System view

Parameters

channel: Sets the channel through which information outputs to the log buffer.

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

size *buffersize*: Specifies the size of the log buffer (number of messages the buffer holds) you want to display. The *buffersize* argument ranges from 0 to 1,024 and defaults to 512.

Description

Use the **info-center logbuffer** command to enable information output to the log buffer.

Use the **undo info-center logbuffer** command to disable information output to the log buffer.

By default, information output to the log buffer is enabled with channel 4 (logbuffer) as the default channel and a maximum buffer size of 512.

This command works only when the information center is enabled.

Related commands: **info-center enable**, **display info-center**.

Examples

Configure the system to output information to the log buffer with the size of 50.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center logbuffer size 50
```

info-center loghost

Syntax

info-center loghost *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*]*

undo info-center loghost *host-ip-addr*

View

System view

Parameters

host-ip-addr: IP address of a log host.

channel: Sets the information channel for the log host.

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

facility: Configures the device name (facility value) for the log host.

local-number: Facility (device name) of the log host, ranging from local0 to local7, and the default setting is local7.

Description

Use the **info-center loghost** command to enable information output to a log host through specifying the IP address of the log host.

Use the **undo info-center loghost** command to disable information output to the log host.

By default, the switch does not output information to the log host. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

This command works only when the information center is enabled.

Note

Be sure to set the correct IP address in the **info-center loghost** command. A loopback IP address will cause an error message, prompting that the address is invalid.

Related commands: **info-center enable**, **display info-center**.

Examples

Configure the system to output system information to the Unix log host whose IP address is 202.38.160.1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center loghost 202.38.160.1
```

info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

View

System view

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Description

Use the **info-center loghost source** command to configure the source interface through which information is sent to the log host.

Use the **undo info-center loghost source** command to cancel the source interface configuration.

Related commands: **info-center enable**, **display info-center**.

Examples

Configure VLAN-interface 1 as the source interface through which information is sent to the log host.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center loghost source Vlan-interface 1
```

info-center monitor channel

Syntax

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

View

System view

Parameters

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description

Use the **info-center monitor channel** command to set the channel through which information is output to user terminals.

Use the **undo info-center monitor channel** command to restore the default channel through which information is output to user terminals.

By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.

This command works only when the information center is enabled.

Related commands: **info-center enable**, **display info-center**.

Examples

Set the system to output information to user terminals through channel 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center monitor channel 0
```

info-center snmp channel

Syntax

info-center snmp channel { *channel-number* | *channel-name* }

undo info-center snmp channel

View

System view

Parameters

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description

Use the **info-center snmp channel** command to set the channel through which information is output to the SNMP agent.

By default, output of system information to the SNMP NMS is enabled with a default channel name of snmpagent and a default channel number of 5.

Related commands: **snmp-agent**, **display info-center**.

Examples

Set the switch to output information to the SNMP agent through channel 6.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center snmp channel 6
```

info-center source

Syntax

info-center source { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*

undo info-center source { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

View

System view

Parameters

modu-name: Module name.

default: Defaults the settings of all modules.

channel-number: Number of information channel to be used.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

log: Specifies to output log information.

trap: Specifies to output trap information.

debug: Specifies to output debugging information.

level *severity*: Specifies an information severity level. For the value of *severity*, refer to Table 1-2.

state *state*: Configures whether to output the system information. The value of *state* can be **on** (enabled) or **off** (disabled).

Description

Use the **info-center source** command to specify the output rules of the system information.

Use the **undo info-center source** command to remove the specified output rules.

By default, the output rules for the system information are listed in Table 1-4.

This command can be used to set the filter and redirection rules of log, trap and debugging information.

For example, the user can set to output log information with severity higher than warnings to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output destination.

Note that:

- If you do not use the *module-name* argument to set output rules for a module, the module uses the default output rules or the output rules set by the **default** keyword; otherwise, the module uses the output rules separately set for it.
- If you use the *module-name* argument to set the output rules for a module without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the module are as follows: the output of log and trap information is enabled, with severity being informational; the output of debugging information is disabled, with severity being debugging. For example, if you execute the command **info-center source snmp channel** 5, the command is actually equal to the command **info-center source snmp channel 5 debug level debugging state off log level informational state on trap level informational state on**.
- After you separately set the output rules for a module, you must use the *module-name* argument to modify or remove the rules. The new configuration by using the **default** keyword is invalid on the module.
- You can configure to output the log, trap and debugging information to the trap buffer, but the trap buffer only receives the trap information and discards the log and debugging information.
- You can configure to output the log, trap and debugging information to the log buffer, but the log buffer only receives the log and debugging information and discards the trap information.
- You can configure to output the log, trap and debugging information to the SNMP module, but the SNMP module only receives the trap information and discards the log and debugging information.

Table 1-4 Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/ disabled	Severity	Enabled/ disabled	Severity	Enabled/ disabled	Severity
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/ disabled	Severity	Enabled/ disabled	Severity	Enabled/ disabled	Severity
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP module	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging

Examples

Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergencies**. Log information of other modules cannot be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent log state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergencies**. Log information of other modules and all the other system information cannot be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent debug state off log state off trap state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

View

System view

Parameters

None

Description

Use the **info-center synchronous** command to enable synchronous information output, so that if system information (such as log information) is output when the user is inputting information, the

command prompt and the input information are echoed after the output (note that, the command prompt is echoed in command edit state but is not echoed in interactive state).

Use the **undo info-center synchronous** command to disable synchronous information output.

By default, the synchronous information output function is disabled.

Note

- The synchronous information output function is used in the case that your input is interrupted by a large amount of system output. With this function enabled, the system echoes your previous input and you can continue your operations from where you were stopped.
- Running the **info-center synchronous** command during debugging information collection may result in a command prompt echoed after each item of debugging information. To avoid unnecessary output, it is recommended to disable synchronous information output in such case.

Examples

Enable synchronous information output.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]info-center synchronous
 Current IC terminal output sync is on
```

info-center timestamp

Syntax

info-center timestamp { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }

undo info-center timestamp { **log** | **trap** | **debugging** }

View

System view

Parameters

log: Specifies log information.

trap: Specifies trap information.

debugging: Specifies debugging information.

boot: Specifies to adopt the time elapsed since system boot, which is in the format of “xxxxxx.yyyyyy”, where xxxxxx is the high 32 bits and yyyyyy the low 32 bits of the elapsed milliseconds.

date: The current system date and time, in the format of “Mmm dd hh:mm:ss:sss yyyy”.

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example “ 7”.
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.

- yyyy: Represents the year.

none: Specifies not to include time stamp in the specified output information.

Description

Use the **info-center timestamp** command to set the format of time stamp included in the log/trap/debugging information.

Use the **undo info-center timestamp** command to restore the default setting of time stamp format.

By default, the **date** time stamp is adopted for log and trap information, and the **boot** time stamp is adopted for debugging information.

Examples

Set the **boot** time stamp for debugging information.

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

info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **no-year-date** | **none** }

undo info-center timestamp loghost

View

System view

Parameters

date: Specifies to adopt the current system date and time, in the format of Mmm dd hh:mm:ss:ms yyyy.

no-year-date: Specifies to adopt the current system date and time excluding the year, in the format of Mmm dd hh:mm:ss:ms.

none: Specifies not to include time stamp in the output information.

Description

Use the **info-center timestamp loghost** command to set the format of time stamp for the output information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default setting of time stamp format.

By default, the **date** time stamp is adopted.

Examples

Set the **no-year-date** time stamp for the output information sent to the log host.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center timestamp loghost no-year-date
```

info-center timestamp utc

Syntax

info-center timestamp utc

undo info-center timestamp utc

View

System view

Parameters

None

Description

Use the **info-center timestamp utc** command to configure to add UTC time zone to the time stamp of the date type output in each direction of the information center.

Use the **undo info-center timestamp utc** command to restore the default.

By default, the information center does not add UTC time zone to the time stamp of the date type in any output direction.

Related commands: **display info-center**, **info-center timestamp**, **info-center timestamp loghost**, **clock timezone**.

Examples

Configure to add UTC time zone to the time stamp of the output information of the information center.

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

Display the time stamp configuration of the information center.

```
[Sysname] display info-center
Information Center: enabled
Log host:
         192.168.0.10, channel number : 2, channel name : loghost
         language : english, host facility local : 7
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 : 153, channel number : 4, channel name : logbuffer
         dropped messages : 0, overwritten messages : 0
Trap buffer:
         enabled,max buffer size : 1024, current buffer size : 256,
         current messages : 1, channel number : 3, channel name : trapbuffer
         dropped messages : 0, overwritten messages : 0
```

```
Information timestamp setting:
         with utc
         log - date, trap - date, debug - boot
```

If you configure to add the UTC time zone in the time stamp, the system information is output as follows:

```
%Dec  8 10:12:21:708 2006 [GMT+08:00:00] Sysname SHELL/5/LOGIN:- 1 - VTY(1.1.0.2) in unit1
login
```

info-center trapbuffer

Syntax

info-center trapbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*

undo info-center trapbuffer [**channel** | **size**]

View

System view

Parameters

size: Sets the size of the trap buffer.

buffersize: Size of the trap buffer, represented by the number of messages it holds. It ranges from 0 to 1,024 and defaults to 256.

channel: Sets the channel through which information is output to the trap buffer.

channel-number: Channel number, ranging from 0 to 9, corresponding to the 10 channels of the system.

channel-name: Channel name. By default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description

Use the **info-center trapbuffer** command to enable information output to the trap buffer.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

This command takes effect only after the information center function is enabled.

Related commands: **info-center enable**, **display info-center**.

Examples

Enable the system to output trap information to the trap buffer, whose size is set to 30.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] info-center trapbuffer size 30
```

reset logbuffer

Syntax

reset logbuffer [**unit** *unit-id*]

View

User view

Parameters

unit-id: Unit ID of the device, the value is 1.

Description

Use the **reset logbuffer** command to clear information recorded in the log buffer.

Examples

Clear information recorded in the log buffer.

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer [**unit** *unit-id*]

View

User view

Parameters

unit-id: Unit ID of the device, the value is 1.

Description

Use the **reset trapbuffer** command to clear information recorded in the trap buffer.

Examples

Clear information recorded in the trap buffer.

```
<Sysname> reset trapbuffer
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Parameters

None

Description

Use the **terminal debugging** command to enable debugging terminal display.

Use the **undo terminal debugging** command to disable debugging terminal display.

By default, debugging terminal display is disabled.

You can execute the **terminal debugging** command to display debugging information on a user terminal.

Related commands: **debugging** commands in the System Maintenance and Debugging module of the manual.

Examples

Enable debugging terminal display.

```
<Sysname> terminal debugging
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Parameters

None

Description

Use the **terminal logging** command to enable log terminal display.

Use the **undo terminal logging** command to disable log terminal display.

By default, log terminal display is enabled for console users and terminal users.

Examples

Disable log terminal display.

```
<Sysname> undo terminal logging
```

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Parameters

None

Description

Use the **terminal monitor** command to enable the debugging/log/trap information terminal display function.

Use the **undo terminal monitor** command to disable the function.

By default, this function is enabled for console users and terminal users.

This command works only on the current terminal. The debugging/log/trap information can be output on the current terminal only after this command is executed in user view.

- Disabling the function has the same effect as executing the following three commands: **undo terminal debugging**, **undo terminal logging** and **undo terminal trapping**. That is, no debugging/log/trap information will be displayed on the current terminal.
- If the function is enabled, you can run the **terminal debugging/undo terminal debugging**, **terminal logging/undo terminal logging** or **terminal trapping/undo terminal trapping** command to enable or disable debug/log/trap terminal output respectively.

Examples

Disable terminal display.

```
<Sysname> undo terminal monitor
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Parameters

None

Description

Use the **terminal trapping** command to enable trap terminal display.

Use the **undo terminal trapping** command to disable trap terminal display.

By default, trap terminal display is enabled.

Examples

Enable trap terminal display.

```
<Sysname> terminal trapping
```

Table of Contents

1 Basic System Configuration and Debugging Commands

Basic System Configuration Commands

clock datetime

Syntax

clock datetime *HH:MM:SS* { *YYYY/MM/DD* | *MM/DD/YYYY* }

View

User view

Parameters

HH:MM:SS: Current time, where *HH* ranges from 0 to 23, *MM* and *SS* range from 0 to 59.

YYYY/MM/DD or *MM/DD/YYYY*: Current date, where *YYYY* represents year ranging from 2000 to 2099, *MM* represents month ranging from 1 to 12, and *DD* represents day ranging from 1 to 31.

Description

Use the **clock datetime** command to set the current date and time of the Ethernet switch.

By default, it is 23:55:00 04/01/2000 when the system starts up.

In an implementation where exact absolute time is required, it is necessary to use this command to set the current date and time of the Ethernet switch.

Related commands: **display clock**.

Examples

Set the current date and time of the Ethernet switch to 0:0:0 2001/01/01.

```
<Sysname> clock datetime 0:0:0 2001/01/01
<Sysname> display clock
00:00:04 UTC Mon 01/01/2001
Time Zone : add 00:00:00
```

clock summer-time

Syntax

clock summer-time *zone-name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*

undo clock summer-time

View

User view

Parameters

zone-name: Name of the summer time, a string of 1 to 32 characters.

one-off: Sets the summer time for only one year (the specified year).

repeating: Sets the summer time for every year starting from the specified year.

start-time: Start time of the summer time, in the form of HH:MM:SS.

start-date: Start date of the summer time, in the form of YYYY/MM/DD or MM/DD/YYYY.

end-time: End time of the summer time, in the form of HH:MM:SS.

end-date: end date of the summer time, in the form of YYYY/MM/DD or MM/DD/YYYY.

offset-time: Offset of the summer time relative to the standard time, in the form of HH:MM:SS.

Description

Use the **clock summer-time** command to set the name, time range and time offset of the summer time.

After the setting, you can use the **display clock** command to check the results.

Examples

Set the summer time named abc1, which starts from 06:00:00 2005/08/01, ends until 06:00:00 2005/09/01, and is one hour ahead of the standard time.

```
<Sysname> clock summer-time abc1 one-off 06:00:00 08/01/2005 06:00:00 09/01/2005 01:00:00
<Sysname> display clock
00:02:36 UTC Mon 01/01/2001
Time Zone : add 00:00:00
Summer-Time : abc1 one-off 06:00:00 08/01/2005 06:00:00 09/01/2005  01:00:00
```

Set the summer time named abc2, which starts from 06:00:00 08/01, ends until 06:00:00 09/01, and is one hour ahead of the standard time every year from 2005 on.

```
<Sysname> clock summer-time abc2 repeating 06:00:00 08/01/2005 06:00:00 09/01/2005 01:00:00
<Sysname> display clock
00:01:25 UTC Mon 01/01/2001
Time Zone : add 00:00:00
Summer-Time : abc2 repeating 06:00:00 08/01/2005 06:00:00 09/01/2005  01:00:00
```

clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *HH:MM:SS*

undo clock timezone

View

User view

Parameters

zone-name: Name of the time zone, in length of 1 to 32 characters.

add: Specifies to add a time value based on the universal time coordinated (UTC) time to generate a later time.

minus: Specifies to subtract a time value based on the UTC time to generate an earlier time.

HH:MM:SS: Time to be added or subtracted from the UTC time, in the form of HH:MM:SS.

Description

Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

After the setting, you can use the **display clock** command to check the setting. The log information time and the debugging information time adopts the local time after the time zone and the summer time have been adjusted.

Related commands: **clock summer-time**, **display clock**.

Examples

Set the local time zone named z5, which is five hours earlier than the UTC time.

```
<Sysname> clock timezone z5 add 05:00:00
<Sysname> display clock
05:03:17 z5 Mon 01/01/2001
Time Zone : z5 add 05:00:00
Summer-Time : abc1 one-off 06:00:00 08/01/2005 06:00:00 09/01/2005  01:00:00
```

quit

Syntax

quit

View

Any view

Parameters

None

Description

Use the **quit** command to return from current view to a lower level view.

The following lists the three levels of views available on a switch (from lower level to higher level):

- User view
- System view
- VLAN view, Ethernet port view, and so on

If the current view is user view, this command is used to quit the system.

Related commands: **return**, **system-view**.

Examples

Return from system view to user view.

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

```
[Sysname] quit
<Sysname>
```

Return to system view from Ethernet port view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname]
```

return

Syntax

return

View

Views other than user view

Parameters

None

Description

Use the **return** command to return from current view to user view. The composite key <Ctrl+Z> has the same effect with the **return** command.

Related commands: **quit**.

Examples

Return from interface view to user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] return
<Sysname>
```

sysname

Syntax

sysname *sysname*

undo sysname

View

System view

Parameters

sysname: System name of the Ethernet switch. It is a string of 1 to 30 characters. By default, it is 3Com.

Description

Use the **sysname** command to set the system name of an Ethernet switch. Use the **undo sysname** command to restore the default system name of the Ethernet switch.

Changing the system name will affect the CLI prompt. For example, if the system name of the switch is 3Com, the prompt for user view is <3Com>.

Examples

Set the system name of the Ethernet switch to **LANSwitch**.

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

system-view

Syntax

system-view

View

User view

Parameters

None

Description

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

Related commands: **quit**, **return**.

Examples

Enter system view from user view.

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

System Status and Information Display Commands

display clock

Syntax

display clock

View

Any view

Parameters

None

Description

Use the **display clock** command to display the current date, time, timezone and summertime of the system, so that you can adjust them if they are wrong.

The maximum date and time that can be displayed by this command is 23:59:59 9999/12/31.

Related commands: **clock datetime**, **clock timezone**, **clock summer-time**.

Examples

Display the current date and time of the system.

```
<Sysname> display clock
18:36:31 beijing Sat 2002/02/02
Time Zone : beijing add 01:00:00
Summer-Time : bj one-off 01:00:00 2003/01/01 01:00:00 2003/08/08 01:00:00
```

Table 1-1 Field description of the **display clock** command

Field	Description
18:36:31 beijing Sat 2002/02/02	Current date and time of the system
Time Zone	Configured time zone information
Summer-Time	Configured summer time information

display debugging

Syntax

display debugging [**unit** *unit-id*] [**interface** *interface-type interface-number*] [*module-name*]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

interface-type: Interface type.

interface-number: Interface number.

module-name: Functional module name.

Description

Use the **display debugging** command to display enabled debugging on a specified device.

Examples

Display enabled debugging on unit 1.

```
<Sysname> display debugging unit 1
ARP packet debugging switch is on
TCP:
  TCP packet debugging switch is on for task any socket any
IP icmp debugging is on
```

display version

Syntax

display version

View

Any view

Parameters

None

Description

Use the **display version** command to display the version information about the switch system.

Specifically, you can use this command to check the software version and release time, the basic hardware configuration, and some other information about the switch.

Examples

Display the version information of the system.

```
<Sysname> display version
3Com Corporation
Switch 4200G 12-Port Software Version 3Com OS V3.02.01s168
Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
Switch 4200G 12-Port uptime is 0 week, 0 day, 11 hours, 30 minutes

Switch 4200G 12-Port with 1 Processor
64M   bytes DRAM
16M   bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.B
CPLD Version is 002
Bootrom Version is 2.00
[SubSlot 0] 12 GE ( 4 COMBO ) Hardware Version is REV.B
```

System Debugging Commands

debugging

Syntax

debugging *module-name* [*debugging-option*]

undo debugging { **all** | *module-name* [*debugging-option*] }

View

User view

Parameters

module-name: Module name.

debugging-option: Debugging option.

all: Specifies to disable all debugging.

Description

Use the **debugging** command to enable system debugging.

Use the **undo debugging** command to disable system debugging.

By default, all debugging is disabled for the system.

Note that:

- Enabled debugging will generate a great deal of debugging information and thus will affect the efficiency of the system. Therefore, it is recommended not to enable debugging for multiple functions at the same time. To disable all debugging at a time, you can use the **undo debugging all** command.
- The specific debugging information can be displayed on a terminal only after you have configured the **debugging**, **terminal debugging**, and **terminal monitor** commands.
- To display the enabled debugging types, use the **display debugging** command.

For information about the **terminal monitor** command, refer to *Information Center Command*.

Examples

Enable packet debugging of the IP module.

```
<Sysname> debugging ip packet
<Sysname> display debugging
IP packet debugging is on
```

display diagnostic-information

Syntax

display diagnostic-information

View

Any view

Parameters

None

Description

Use the **display diagnostic-information** command to display system diagnostic information, or save system diagnostic information to a file with the extension .diag in the Flash memory.

Examples

Save system diagnostic information to the file **default.diag**.

```
<Sysname> display diagnostic-information
 This operation may take a few minutes, continue?[Y/N]y
 Diagnostic-information is saved to Flash or displayed(Y=save N=display)?[Y/N]y
 Please input the file name(*.diag)[flash:/default.diag]:
 The file is already existing, overwrite it? [Y/N]y
```

```
% Output information to file: flash:/default.diag.
Please wait......
```

Display the diagnostic information of the system.

```
<Sysname> display diagnostic-information
 This operation may take a few minutes, continue?[Y/N]y
 Diagnostic-information is saved to Flash or displayed(Y=save N=display)?[Y/N]n

-------------------- display version --------------------
……
<Omitted>
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Parameters

None

Description

Use the **terminal debugging** command to enable terminal display for debugging information.

Use the **undo terminal debugging** command to disable terminal display for debugging information.

By default, terminal display for debugging information is disabled.

Note that:

- To display the debugging information on the terminal, you need to configure both the **terminal debugging** and **terminal monitor** commands.
- If you execute the **undo terminal monitor** command, you will disable the monitoring of the log, trap, and debugging information on the current terminal. Thereby, no log, trap, or debugging information will be displayed on the terminal.
- The configuration of the **terminal debugging** command takes effect for the current connection only. If the terminal re-establishes a connection, the terminal display for debugging information is disabled.

Related commands: **debugging**.

Examples

Enable terminal display for debugging information.

```
<Sysname> terminal debugging
% Current terminal debugging is on
```

2 Network Connectivity Test Commands

Network Connectivity Test Commands

ping

Syntax

ping [-**a** *ip-address*] [**-c** *count*] [**-d**] [**-f**] [**-h** *ttl*] [**-i** *interface-type interface-number*] [**ip**] [**-n**] [**- p** *pattern*] [**-q**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*

View

Any view

Parameters

-a *ip-address*: Specifies the source IP address to send ICMP ECHO-REQUEST packet. This IP address must be a local interface IP address.

-c *count*: Specifies how many times the ICMP ECHO-REQUEST packet will be sent. The *count* argument is the times, which ranges from 1 to 4,294,967,295 and defaults to 5.

-d: Specifies the socket to be in DEBUGGING mode. By default, the socket is in non-DEBUGGING mode.

-f: Specifies to discard a packet directly instead of fragmenting it if its length is greater than the maximum transmission unit (MTU) of the interface.

-h *ttl*: Specifies the Time To Live (TTL) value of the ICMP ECHO-REQUEST packets in the range 1 to 255. By default, the TTL value is 255.

-i *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number. With the interface specified, the TTL of packets are set to 1 automatically to test the directly-connected device (the IP address of the device is in the same network segment with that of the interface).

ip: Specifies the device to support IPv4. By default, the device supports IPv4.

-n: Specifies to directly regard the *host* argument as an IP address without performing domain name resolution. By default, the *host* argument is first regarded as an IP address; if it is not an IP address, domain name resolution is performed.

-p *pattern*: Specifies the padding byte pattern of the ICMP ECHO-REQUEST packets. The *pattern* argument is a byte in hexadecimal. For example, **-p** ff fills a packet with all ffs. By default, the system fills a packet with 0x01, 0x02, and so on, until 0x09; then it repeats this procedure from 0x01 again.

-q: Specifies to display only the statistics without the details. By default, all the information including the details and statistics will be displayed.

-s *packetsize*: Specifies the size (in bytes) of each ICMP ECHO-REQUEST packet (excluding the IP and ICMP headers). The *packetsize* argument ranges from 20 to 32,000 and defaults to 56 bytes.

-t *timeout*: Specifies the timeout time (in milliseconds) before an ICMP ECHO-REPLY packet is received after an ICMP ECHO-REQUEST packet is sent. The *timeout* argument ranges from 0 to 65535 ms and defaults to 2,000 ms.

-tos *tos*: Specifies the ToS value of the ICMP ECHO-REQUEST packets in the range 0 to 255. By default, this value is 0.

-v: Specifies to display other ICMP packets received (that is, non-ECHO-REPLY packets). By default, other ICMP packets like non-ECHO-REPLY packets are not displayed.

host: Domain name or IP address of the destination host.

Note

The **ping** command also supports the **ipv6** keyword. For details, refer to *IPv6 Management Command*.

Description

Use the **ping** command to check the reachability of a host, and output the related statistics information.

The executing procedure of the **ping** command is as follows: First, the source host sends an ICMP ECHO-REQUEST packet to the destination host. If the connection to the destination network is normal, the destination host receives this packet and responds with an ICMP ECHO-REPLY packet.

You can use the **ping** command to check the network connectivity and the quality of a network line. This command can output the following information:

- Response status of the destination to each ICMP ECHO-REQUEST packet, including the number of bytes, packet sequence number, TTL and response time of the response packet if the response packet is received within the timeout time. If no response packet is received within the timeout time, the message "Request time out" is displayed instead.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

You can set a relatively long timeout time if the network transmission speed is slow.

Related commands: **tracert**.

Examples

Check the reachability of the host whose IP address is 202.38.160.244.

```
<Sysname> ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes, press CTRL_C to break
Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packet transmitted
5 packet received
```

```
0% packet loss
round-trip min/avg/max = 1/2/3 ms
```

The above output information indicates that the destination host is reachable. Each probe packet from the source device has got a reply, with the minimum/average/maximum packet roundtrip time being 1ms/2ms/3ms.

tracert

Syntax

tracert [**-a** *source-ip*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *num-packet*] [**-w** *timeout*] *string*

View

Any view

Parameters

-a *source-ip*: Specifies the source interface IP address used by this command.

-f *first-ttl*: Specifies the initial TTL value of the packets to be sent, so as to only display the addresses of those gateways on the path whose hop counts are not smaller than the hop count specified by the *first-ttl* argument. For example, if the *first-ttl* argument is 3, the command displays the addresses of the gateways from the third hop. The *first-ttl* argument ranges from 1 to 255 and defaults to 1.

-m *max-ttl*: Specifies the maximum TTL value of the packets to be sent. After the command sends a packet with the maximum TTL, it will not send any more packets. With this argument, this command only displays the addresses of those gateways from the source address to hop according to the hop count specified by the argument. For example, if the *max-ttl* argument is 5, the command displays the addresses of the gateways from the source to the fifth hop. The *max-ttl* argument ranges from 1 to 255 and defaults to 30.

-p *port*: Specifies the destination port of the packets to be sent. The *port* argument ranges from 0 to 65535 and defaults to 33434. Generally, you need not change the argument.

-**q** *num-packet*: Specifies the number of packets to be sent each time. The *num-packet* argument ranges from 0 to 65,535 and defaults to 3.

-w *timeout*: Specifies the timeout time to wait for ICMP error packets. The *timeout* argument ranges from 0 to 65,535 and defaults to 5,000 (in milliseconds).

string: IP address of the destination host, or host name of the remote system with 1 to 20 characters.

Note

The **tracert** command also supports the **ipv6** keyword. For details, refer to *IPv6 Management Command*.

Description

Use the **tracert** command to trace the gateways that the test packets pass through from the source device to the destination device. This command is mainly used to check the network connectivity and help locate the network faults.

The executing procedure of the **tracert** command is as follows: First, the source sends a packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source resends a packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until a packet gets to the destination or the maximum TTL is reached. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packets pass through to the destination.

If you find that the network is faulty by using the **ping** command, you can use the **tracert** command to find where the fault is in the network.

The **tracert** command can output the IP addresses of all the gateways that the packets pass through to the destination. It outputs the string "***" if the response from a gateway times out.

Examples

Trace the gateways that the packets pass through to the destination with IP address 18.26.0.115.

```
<Sysname> tracert 18.26.0.115
tracert to 18.26.0.115 (18.26.0.115), 30 hops max,40 bytes packet
1 128.3.112.1 (128.3.112.1) 0 ms 0 ms 0 ms
2 128.32.216.1 (128.32.216.1) 19 ms 19 ms 19 ms
3 128.32.206.1 (128.32.206.1) 39 ms 19 ms 19 ms
4 128.32.136.23 (128.32.136.23) 19 ms 39 ms 39 ms
5 128.32.168.22 (128.32.168.22) 20 ms 39 ms 39 ms
6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 18.26.0.115 (18.26.0.115) 339 ms 279 ms 279 ms
```

3 Device Management Commands

Device Management Commands

boot boot-loader

Syntax

boot boot-loader [**backup-attribute**] { *file-url* | *device-name* }

View

User view

Parameters

backup-attribute: Specifies the backup attribute for a file.

file-url: Path plus name of a host software file in the Flash, a string of 1 to 64 characters.

device-name: File name, in the form of **unit[NO.]>flash:**, which is used to indicate that the specified file is stored in the Flash memory of a specified switch.

Description

Use the **boot boot-loader** command to specify the host software that will be used when the switch starts up next time.

You can use this command to specify a .app file in the Flash as the host software to be adopted at next startup.

Examples

Specify the host software that will be used when the current switch starts up next time.

```
<Sysname> boot boot-loader S4200G.app
The specified file will be booted next time on unit 1!
```

boot bootrom

Syntax

boot bootrom { *file-url* | *device-name* }

View

User view

Parameters

file-ulr: Path plus name of a Boot ROM file (that is, a .btm file) in the Flash, a string of 1 to 64 characters.

device-name: File name, beginning with a device name in the form of **unit[NO.]>flash**, used to indicates that the specified file is stored in the Flash memory of a specified switch.

Description

Use the **boot bootrom** command to update the Boot ROM. The updated Boot ROM is used at next startup.

Examples

Update the Boot ROM of the switch using the file named S4200G.btm.

```
<Sysname> boot bootrom S4200G.btm
 This will update Bootrom on unit 1.  Continue? [Y/N] y
 Upgrading Bootrom, please wait...
 Upgrade Bootrom succeeded!
```

display boot-loader

Syntax

display boot-loader [**unit** *unit-id*]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

Description

Use the **display boot-loader** command to display the host software (.app file) that will be adopted when the switch starts up next time.

Examples

Display the host software that will be adopted when the switch starts up next time.

```
<Sysname> display boot-loader
 Unit 1:
   The current boot app is: s4200G.app
   The main boot app is:    s4200G.app
   The backup boot app is:
```

Table 3-1 Description for the fields of the **display boot-loader** command

Field	Description
The current boot app is	Boot file used for the current boot of the system
The main boot app is	Main boot file to be used for the next boot of the system
The backup boot app is	Backup boot file to be used for the next boot of the system

display cpu

Syntax

display cpu [**unit** *unit-id*]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

Description

Use the **display cpu** command to display the CPU usage.

Examples

Display the CPU usage of this switch.

```
<Sysname> display cpu
Unit 1
Board 0 CPU busy status:
    12% in last 5 seconds
    12% in last 1 minute
    12% in last 5 minutes
```

Table 3-2 Description for the fields of the **display cpu** command

Field	Description
CPU busy status	CPU usage status.
12% in last 5 seconds	The CPU usage in the last five seconds is 12%.
12% in last 1 minute	The CPU usage in the last one minute is 12%.
12% in last 5 minutes	The CPU usage in the last five minutes is 12%.

display device

Syntax

display device [**manuinfo** | **unit** *unit-id*]

View

Any view

Parameters

manuinfo: Specifies to display the manufacture information of the specified switch.

unit-id: Unit ID of a switch, the value is 1.

Description

Use the **display device** command to display the information, such as the module type and operating status, about each board (main board and sub-board) of a specified switch.

You can use this command to display the following information about each board, including slot number, sub-slot number, the number of ports, versions of PCB, FPGA, CPLD and Boot ROM software, address learning mode, interface board type, and so on.

Examples

Display board information of this switch.

```
<Sysname> display device
Unit 1
SlotNo SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      0      48      REV.B  NULL    002     2.00       IVL    MAIN       Normal
```

Table 3-3 Description on the fields of the **display device** command

Field	Description
SlotNo	Serial number of the slot
SubSNo	Serial number of the sub slot
PortNum	Number of ports
PCBVer	Version number of the PCB card
FPGAVer	Version number of the FPGA encapsulation
CPLDVer	Logical version number of the hardware CPLD
BootRomVer	Version number of the Boot ROM
AddrLM	MAC address learning mode
Type	Card type
State	Running state

display fan

Syntax

display fan [**unit** *unit-id* [*fan-id*]]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

fan-id: ID number of a fan.

Description

Use the **display fan** command to view the working states of fans in a switch.

Examples

Display the working states of the fans.

```
<Sysname> display fan
Unit 1
 Fan  1 State: Normal
 Fan  2 State: Normal
 Fan  3 State: Normal
```

The above information indicates that the three fans work normally.

display memory

Syntax

display memory [**unit** *unit-id*]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

limit: Specifies to display the memory configuration information of the switch.

Description

Use the **display memory** command to display the memory usage of a specified switch.

Examples

Display the memory usage of this switch.

```
<Sysname> display memory
Unit 1
System Available Memory(bytes): 27460224
System Used Memory(bytes): 10900616
Used Rate: 39%
```

Table 3-4 Description for the fields of the **display memory** command

Field	Description
System Available Memory(bytes)	Available memory size of the system, in unit of bytes
System Used Memory(bytes)	Used memory size of the system, in unit of bytes
Used Rate	Percentage of the used memory

display power

Syntax

display power [**unit** *unit-id* [*power-id*]]

View

Any view

Parameters

unit-id: Unit ID of a switch, the value is 1.

power-id: Power ID.

Description

Use the **display power** command to display the working state of the power supply of the switch.

Examples

Display the working state of the power supply.

```
<Sysname> display power
Unit 1
  power    1
  State    : Normal
  Type     : AC
```

The above information indicates that the power supply type is AC, and works normally.

display schedule reboot

Syntax

display schedule reboot

View

Any view

Parameters

None

Description

Use the **display schedule reboot** command to display information about scheduled reboot.

Related commands: **schedule reboot at**, **schedule reboot delay**.

Examples

Display the information about scheduled reboot.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 2002/11/1 (in 2 hours and 5 minutes).
```

display transceiver alarm interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display transceiver alarm interface** command to display the current alarm information of a single or all transceivers.

If no error occurs, **None** is displayed.

Table 3-5 shows the alarm information that may occur for the four types of transceivers.

Table 3-5 Description on the fields of display transceiver alarm interface

Field	Remarks
GBIC/SFP	
RX loss of signal	RX signal is lost.
RX power high	RX power is high.
RX power low	RX power is low.
TX fault	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	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.
XENPAK	
WIS local fault	WIS (WAN Interface Sublayer) local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	PMA/PMD (Physical Medium Attachment/Physical Medium Dependent) receiver local fault
PCS receive local fault	PCS (Physical Coding Sublayer) receiver local fault
PHY XS receive local fault	PHY XS (PHY Extended Sublayer) receive local fault
RX power high	RX power is high.
RX power low	RX power is low.
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD receiver local fault	PMA/PMD receiver local fault
PCS receive local fault	PCS receive local fault
PHY XS receive local fault	PHY XS receive local fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.

Field	Remarks
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.

Examples

Display the alarm information of the transceiver on interface GigabitEthernet 1/0/50.

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/50
GigabitEthernet1/0/50 transceiver current alarm information:
  TX fault
```

Table 3-6 Description on the fields of display transceiver alarm interface

Field	Description
transceiver current alarm information	Current alarm information of the transceiver
TX fault	TX fault

display transceiver diagnosis interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display transceiver diagnosis interface** command to display the currently measured value of digital diagnosis parameters of a single or all anti-spoofing transceivers customized by H3C.

Examples

Display the currently measured value of digital diagnosis parameters of the anti-spoofing pluggable optical transceiver customized by H3C on interface GigabitEthernet 1/0/50.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/50
GigabitEthernet1/0/50 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 3-7 Description on the fields of display transceiver diagnosis interface

Field	Description
transceiver diagnostic information	Digital diagnosis information of the transceiver carried by an interface

Field	Description
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 interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display transceiver interface** command to display main parameters of a single or all transceivers.

Examples

Display main parameters of the pluggable transceiver on interface GigabitEthernet 1/0/50.

```
<Sysname> display transceiver interface gigabitethernet 1/0/50
GigabitEthernet1/0/50 transceiver information:
  Transceiver Type                 : 1000_BASE_LX_SFP
  Connector Type                   : LC
  Wavelength(nm)                   : 1310
  Transfer Distance(km)            : 10(9um)
  Digital Diagnostic Monitoring    : YES
  Vendor Name                      : H3C
  Ordering Name                    : N/A
```

Table 3-8 Description on the fields of the **display transceiver interface** command

Field	Description
transceiver information	Transceiver information of the interface
Transceiver Type	Transceiver type

Field	Description
Connector Type	Type of the connectors of the transceiver: • Optical connectors, including SC (SC connector, developed by NTT) and LC (LC connector, 1.25 mm/RJ45 optical connector developed by Lucent). • Other connectors, including RJ-45 and CX4.
Wavelength(nm)	• Optical transceiver: central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma. • Electrical transceiver: displayed as N/A.
Transfer distance(xx)	Transfer distance, with xx representing km for single-mode transceivers and m for other transceivers. If the transceiver supports multiple transfer medium, every two values of the transfer distance are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the transfer media: • 9 um: 9/125 um single-mode fiber • 50 um: 50/125 um multi-mode fiber • 62.5 um: 62.5/125 um multi-mode fiber • TP: Twisted pair • CX4: CX4 cable
Digital Diagnostic Monitoring	Whether the digital diagnosis function is supported, where: • YES: supported • NO: not supported
Vendor Name	Vendor name or vendor name specified of the transceiver: • The anti-spoofing transceiver customized by H3C: **H3C** is displayed. • Other transceivers: The original vendor name is displayed.
Ordering Name	Ordering name of the transceiver

display transceiver manuinfo interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display transceiver manuinfo interface** command to display part of the electrical label information of a single or all anti-spoofing pluggable transceivers customized by H3C.

Examples

Display part of the electrical label information of the anti-spoofing pluggable transceiver customized by H3C on interface GigabitEthernet 1/0/50.

```
<Sysname> display transceiver manuinfo interface gigabitethernet 1/0/50
```

```
GigabitEthernet1/0/50 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2007-07-28
  Vendor Name          : H3C
```

Table 3-9 Description on the fields of display transceiver manuinfo interface

Field	Description
Manu. Serial Number	Serial number generated during debugging and testing
Manufacturing Date	Debugging and testing date.. The date takes the value of the system clock of the computer that performs debugging and testing.
Vendor Name	Vendor name specified, that is, H3C.

port auto-power-down

Syntax

port auto-power-down

undo port auto-power-down

View

Ethernet port view

Parameters

None

Description

Use the **port auto-power-down** command to enable auto power down on an Ethernet port.

Use the **undo port auto-power-down** to restore the default.

By default, auto power down is not enabled on an Ethernet port.

Note that, currently, in the S4200G series Ethernet switches, the auto power down configuration does not take effect on SFP ports.

Examples

Enable auto power down on GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] port auto-power-down
```

reboot

Syntax

reboot [**unit** *unit-id*]

View

User view

Parameters

unit-id: Unit ID of a switch, the value is 1.

Description

Use the **reboot** command to restart a specified Ethernet switch.

 **Note**

Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations.

Examples

Directly restart this switch without saving the current configuration.

```
<Sysname> reboot
Start to check configuration with next startup configuration file,
 please wait......
 This command will reboot the device. Current configuration will be lost in next startup if
you continue.   Continue? [Y/N] y
 This will reboot device. Continue? [Y/N] y

<Sysname>
%Apr  2 00:06:01:148 2006 Sysname DEV/5/DEV_LOG:- 1 -
Switch is rebooting...

Starting......
```

schedule reboot at

Syntax

schedule reboot at *hh:mm* [*mm/dd/yyyy* | *yyyy/mm/dd*]

undo schedule reboot

View

User view

Parameters

hh:mm: Reboot time, where *hh* (hour) ranges from 0 to 23, and *mm* (minute) ranges from 0 to 59.

mm/dd/yyyy or *yyyy/mm/dd*: Reboot date, where *yyyy* (year) ranges from 2,000 to 2,099, *mm* (month) ranges from 1 to 12, and the range of *dd* (day) depends on the specific month. You cannot set the date 30 days later than the system current date.

Description

Use the **schedule reboot at** command to enable the scheduled reboot function on the current switch and set the reboot date and time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, no scheduled reboot is set on the switch.

Note

The switch timer can be set to a precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

Note that:

- After you execute the **schedule reboot at** command with a specified future date, the switch will reboot at the specified time with at most one minute delay.
- After you execute the **schedule reboot at** command without specifying a date, the switch will reboot at the specified time on the current day if the specified time is later than the current time, or reboot at the specified time on the next day if the specified time is earlier than the current time.
- After you execute the command, the system will prompt you to confirm. Enter "Y" or "y" for your setting to take effect, and your setting will overwrite the previous one (if there is a setting already exists).
- If you adjust the system time by the **clock** command after executing the **schedule reboot at** command, the configured **schedule reboot at** command will be invalid and the scheduled reboot will not happen.

Related commands: **reboot**, **display schedule reboot**.

Examples

Suppose the current time is 05:06, schedule a reboot so that the switch reboots at 22:00 on the current day.

```
<Sysname> schedule reboot at 22:00
Reboot system at 22:00 2000/04/02(in 16 hours and 53 minutes)
confirm?[Y/N]:y
<Sysname>
```

schedule reboot delay

Syntax

schedule reboot delay { *hh:mm* | *mm* }

undo schedule reboot

View

User view

Parameters

hh:mm: Reboot waiting delay, where *hh* ranges from 0 to 720, and *mm* ranges from 0 to 59. The value of *hh:mm* can be up to 720:00.

mm: Reboot waiting delay, ranging from 0 to 43,200 minutes.

Description

Use the **schedule reboot delay** command to enable the delay reboot function on the switch, and set the reboot delay time.

Use the **undo schedule reboot** command to disable the delay reboot function.

By default, the delay reboot function is disabled on the switch.

Note that:

- The switch timer is precise to one minute. When the reboot time reaches, the switch will reboot in one minute at most.
- You can set the reboot delay in two formats: the hour:minute format and the absolute minute format, and both must be less than or equal to 30 × 24 × 60 (that is, 30 days).
- After you execute the command, the system will prompt you to confirm. Enter "Y" or "y" for your setting to take effect. Your setting will overwrite the previous one (if there is a setting already exists).
- If you adjust the system time by the **clock** command after executing the **schedule reboot delay** command, the configured **schedule reboot delay** command will be invalid and the scheduled reboot will not happen.

Related commands: **reboot**, **schedule reboot at**, **undo schedule reboot**, **display schedule reboot**.

Examples

Suppose the current time is 05:02, schedule a reboot so that the switch reboots after 70 minutes.

```
<Sysname> schedule reboot delay 70
Reboot system at 06:12 2000/04/02(in 1 hours and 10 minutes)
confirm?[Y/N]:y
<Sysname>
```

schedule reboot regularity

Syntax

schedule reboot regularity at *hh:mm period*

undo schedule reboot regularity

View

System view

Parameters

hh:mm: Reboot time of the switch, in the hour:minute format, where *hh* ranges from 0 to 24, and *mm* ranges from 0 to 59.

period: Reboot period of the switch, in the format *period* = { **daily** | { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** }* }. **daily** indicates the reboot period is one day, that is, the switch reboots at a specified time every day. { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** }* indicates the week day when the switch reboots.

Description

Use the **schedule reboot regularity** command to enable the periodical reboot of the switch and set the reboot time.

Use the **undo schedule reboot regularity** command to cancel the configured reboot period.

By default, the reboot period of the switch is not configured.

Note

The switch timer can be set to a precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

After you execute the command, the system will prompt you to confirm. Enter "Y" or "y" for your setting to take effect. Your setting will overwrite the previous one (if available).

If you adjust the system time by the **clock** command after executing the **schedule reboot regularity** command, the **schedule reboot regularity** command will be invalid.

Related commands: **reboot**, **schedule reboot at**, **undo schedule reboot**, **display schedule reboot**.

Examples

Schedule a reboot so that the switch reboots at 10:00 every Thursday.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] schedule reboot regularity at 10:00 thursday
Schedule reboot regularity, are you sure?[Y/N]:y
[Sysname]
```

system-monitor enable

Syntax

system-monitor enable

undo system-monitor enable

View

System view

Parameters

None

Description

Use the **system-monitor enable** command to enable real-time monitoring of the running status of the system.

Use the **undo system-monitor enable** command to disable real-time monitoring of the running status of the system.

This function enables you to dynamically record the system running status, such as CPU, thus facilitating analysis and solution of the problems of the device.

By default, real-time monitoring of the running status of the system is enabled.

 **Caution**

Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to save your CPU resources.

Examples

Disable real-time monitoring of the running status of the system.

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

xmodem get

Syntax

xmodem get { *file-url* | *device-name* }

View

User view

Parameters

file-url: Path plus name of a host software file in the Flash, a string of 1 to 64 characters.

device-name: File name, in the form of **unit[NO.]>flash:**, which is used to indicate that the specified file is stored in the Flash of a specified switch.

Description

Use the **xmodem get** command to download files from the local device connected with the Console port of a switch through XModem. This command can be configured only when the device logging onto a switch through the Console port.

Note that, the communication parameter settings of the Console port of the switch and those of the serial port of the local device must be consistent and, the interface type of the Console port must be AUX.

Examples

Download files through XModem.

```
<Sysname> xmodem get flash:/config.cfg
                **** WARNING ****
```

xmodem is a slow transfer protocol limited to the current speed settings of the auxiliary ports.

During the course of the download no exec input/output will be available!

---- ******* ----

Table of Contents

1 VLAN-VPN Configuration Commands

VLAN-VPN Configuration Commands

display port vlan-vpn

Syntax

display port vlan-vpn

View

Any view

Parameter

None

Description

Use the **display port vlan-vpn** command to display the information about VLAN-VPN configuration of the current system. including current TPID value, VLAN-VPN ports, and VLAN-VPN uplink ports.

Example

Display the information about VLAN-VPN configuration of the current system

```
<Sysname> display port vlan-vpn
 VLAN-VPN TPID: 8100

GigabitEthernet1/0/4
 VLAN-VPN status: enabled
 VLAN-VPN VLAN: 1

GigabitEthernet1/0/11
 VLAN-VPN uplink status: enabled

GigabitEthernet1/0/12
 VLAN-VPN uplink status: enabled
```

Table 1-1 Description on the fields of the display port vlan-vpn command

Field	Description
VLAN-VPN status	The operation status of the VLAN VPN feature on the port **enabled** indicates that VLAN VPN is enabled on the port. You can use the **vlan-vpn enable** command to enable VLAN VPN on a port.

Field	Description
VLAN-VPN VLAN	The VLAN corresponding to the tag that the port tags packets with, that is, the default VLAN of the port. For descriptions on default VLAN, refer to *VLAN Operation*.

vlan-vpn enable

Syntax

vlan-vpn enable

undo vlan-vpn

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn enable** command to enable the VLAN-VPN feature for a port.

Use the **undo vlan-vpn** command to disable the VLAN-VPN feature for a port.

By default, the VLAN-VPN feature is disabled.

With the VLAN-VPN feature enabled, a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag.

- If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet.
- Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Caution

- If this port is a remote mirror reflection port, the VLAN-VPN function cannot be enabled on the port.
- If this port is a VLAN-VPN uplink port, the VLAN-VPN function cannot be enabled on the port.

You can use the **display port vlan-vpn** command to display the configuration information of VLAN-VPN on the ports to verity your configuration.

After the VLAN-VPN function is enabled, you can use the **vlan-vpn vid** command and the **raw-vlan-id inbound** command to configure the selective QinQ function. Refer to Selective QinQ Configuration Commands for details.

Example

Enable the VLAN-VPN feature for GigabitEthernet 1/0/1 port.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan-vpn enable
```

vlan-vpn tpid

Syntax

vlan-vpn tpid *value*

undo vlan-vpn tpid

View

System view

Parameter

value: User-defined TPID value (in hexadecimal format), in the range 0x0001 to 0xFFFF.

Description

Use the **vlan-vpn tpid** command to set the TPID value.

Use the **undo vlan-vpn tpid** command to restore the default TPID value.

The default TPID value is 0x8100.

The position of the TPID field in an Ethernet packet is the same as the position of the protocol type field in a packet without VLAN Tag. Thus, to avoid confusion happening when the switch forwards or receives a packet, do not configure the protocol type values listed in Table 1-2 as the TPID value.

Table 1-2 Common Ethernet frame protocol type values

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

Example

Set the TPID value to 0x9100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vlan-vpn tpid 9100
```

vlan-vpn uplink enable

Syntax

vlan-vpn uplink enable

undo vlan-vpn uplink

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn uplink enable** command to configure a port to be a VLAN-VPN uplink port.

Use the **undo vlan-vpn uplink** command to remove the configuration.

By default, no port is configured to VLAN-VPN uplink port.

When sending a VLAN-VPN packet, a VLAN-VPN uplink port replaces the TPID value in the outer VLAN tag of the packet with the customized TPID value. You can use the **vlan-vpn tpid** command to set the TPID value used by the VLAN-VPN uplink port.

Caution

- A port cannot be configured to VLAN-VPN port and VLAN-VPN uplink port at the same time.
- With the TPID being 0x8100, every port can be configured as a VLAN VPN uplink port. However, if the TPID value is not the default value, you need to use the **vlan-vpn uplink enable** command to specify a VLAN VPN uplink port.

Example

Configure GigabitEthernet1/0/2 port to be a VLAN-VPN uplink port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] vlan-vpn uplink enable
```

2 Selective QinQ Configuration Commands

Selective QinQ Configuration Commands

raw-vlan-id inbound

Syntax

raw-vlan-id inbound *vlan-id-list*

undo raw-vlan-id inbound { **all** | *vlan-id-list* }

View

QinQ view

Parameter

vlan-id-list: Lists of VLAN IDs to be tagged as outer VLAN tags. You need to provide this argument in the form of { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the VLAN ID after the **to** keyword must be larger than or equal to the VLAN ID before the **to** keyword and &<1-10> means that you can specify up to 10 VLANs/VLAN ranges for this argument.

all: Removes all configurations of encapsulating an outer VLAN tag for specified inner VLANs in the current view.

Description

Use the **raw-vlan-id inbound** command to specify the outer tag for the packets with the specified inner VLAN tags. This command must be configured on ports receiving packets from the private network.

Use the **undo raw-vlan-id inbound** command to remove the configuration.

By default, the switch does not encapsulate packets with any outer VLAN tag.

Caution

A packet cannot be tagged with different outer VLAN tags. To change the outer VLAN tag of a packet, you need to remove the existing outer VLAN tag configuration and configure a new outer VLAN tag.

Before configuring this command in QinQ view, you need to use the **vlan-vpn vid** command to configure the outer VLAN tag to be used in the selective QinQ policy.

Example

Specify to add the tag of VLAN 20 as the outer tag to the packets with their inner VLAN IDs being 8 through 15 for GigabitEthernet 1/0/1.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan-vpn vid 20
[Sysname-GigabitEthernet1/0/1-vid-20] raw-vlan-id inbound 8 to 15
```

vlan-vpn priority

Syntax

vlan-vpn priority *old-priority* **remark** *new-priority*

undo vlan-vpn priority *old-priority*

View

Ethernet port view

Parameter

old-priority: 802.1p priority of the inner VLAN tag in a packet. This argument can be in the range 0 to 7 or a keyword listed in Table 2-1.

new-priority: Priority for the outer VLAN tag in a packet. This argument can be in the range 0 to 7 or a keyword listed in Table 2-1.

Table 2-1 Description on 802.1p priority

IP Precedence (decimal)	Keyword
0	Best-effort
1	Background
2	Spare
3	Excellent-effort
4	Controlled-load
5	Video
6	Voice
7	Network-management

Note

For the description on the priority values and the keywords listed in Table 2-1, refer to *Qos-QoS profile*.

Description

Use the **vlan-vpn priority** command to configure the mapping between the inner VLAN priority and the outer VLAN priority. With the mapping configured, a port will encapsulate a packet with the specified inner tag priority with an outer tag that has the corresponding priority.

Use the **undo vlan-vpn priority** command to remove the configuration.

By default, no mapping between the inner tag priority and the outer tag priority is configured, and the switch uses the priority of the receiving port as the outer tag priority of packets. For descriptions on receiving port priority, refer to *QoS-QoS Profile Operation*.

Example

Enable the inner-to-outer tag priority mapping feature for GigabitEthernet 1/0/1. Insert outer tags with the priorities being 5 to packets with the priorities of their inner tags being 3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan-vpn priority 3 remark 5
```

vlan-vpn vid

Syntax

vlan-vpn vid *vlan-id*

undo vlan-vpn vid *vlan-id*

View

Ethernet port view

Parameter

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

Description

Use the **vlan-vpn vid** command to configure the outer VLAN tag for a selective QinQ policy (that is, the outer VLAN tag to be used by a port to encapsulate received packets) and to enter QinQ view.

Use the **undo vlan-vpn vid** command to remove the configured outer VLAN tag. Note that this command will also remove all configurations configured by the **raw-vlan-id inbound** command in QinQ view.

Before configuring this command, make sure that the **vlan-vpn enable** command is configured.

Note

- Before configuring this command, make sure that the **vlan-vpn enable** command is configured.
- You are not recommended to configure both the DHCP snooping and selective QinQ function on the switch, which may result in the DHCP snooping to function abnormally.

By default, no selective QinQ policy is configured on a port.

After specifying an outer VLAN tag and enter QinQ view, you need to use the **raw-vlan-id inbound** command to specify which VLANs' packets will be encapsulated with the specified outer VLAN tag. Otherwise, the configuration of the outer VLAN tag is of no use.

Related command: **raw-vlan-id inbound**.

Example

Specify to add VLAN 20 tag as the outer tags to the packets with their inner VLAN IDs being 2 through 14 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan-vpn vid 20
[Sysname-GigabitEthernet1/0/1-vid-20] raw-vlan-id inbound 2 to 1
```

Table of Contents

1 remote-ping Commands

remote-ping Client Commands

adv-factor

Syntax

adv-factor *adv-number*

undo adv-factor

View

remote-ping test group view

Parameters

adv-number: Advantage factor, used to count Mos and ICPIF value in a jitter voice test. It is in the range 0 to 20 and defaults to 0.

Description

Use the **adv-factor** command to configure the advantage factor which is used to count Mos and ICPIF value in a jitter voice test.

Use the **undo adv-factor** command to restore the default.

Note

This command applies only to jitter voice test.

Examples

Configure the advantage factor for a jitter voice test as 10.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator jitter
[Sysname-remote-ping-administrator-jitter] test-type jitter codec g711a
[Sysname-remote-ping-administrator-jitter] adv-factor 10
```

count

Syntax

count *times*

undo count

View

remote-ping test group view

Parameters

times: Number of probes in each remote-ping test. The *times* argument ranges from 1 to 15.

Description

Use the **count** command to set the number of probes in each remote-ping test.

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

For tests except jitter test, only one packet is sent in a probe. In a jitter test, you can use the **jitter-packetnum** command to set the number of packets to be sent in a probe.

By default, the number of probes in each test is 1.

Related commands: **frequency**.

Examples

Set the number of probes made in an ICMP test to 10.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] count 10
```

datafill

Syntax

datafill *string*

undo datafill

View

remote-ping test group view

Parameters

string: Data for padding test packets. It is a string of 1 to 230 characters, including spaces

Description

Use the **datafill** command to configure the data for padding test packets.

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

By default, test packets are padded with characters in the range 0 to 255 cyclically.

You can pad remote-ping test packets with a character string in the range of 1 to 230 characters, including spaces. If the size of a test packet is smaller than that of the configured padding string, only a portion of the data is used. If the size of the packet is larger, the string is used cyclically for padding. Suppose a padding string, “abcd” is configured. If the test packet size is 3 bytes, only “abc” is used; if it is 8 bytes, the string “abcdeabc" is used.

Note that:

- The configuration of a padding character string is only supported by ICMP, UDP and jitter tests.
- A portion of a test packet is reserved and the padding character string is padded to the rest part. The length of the reserved part varies depending on the test type. Table 1-1 describes the reserved length for different test types.

Table 1-1 Reserved length of a packet for different test types

Test type	Code type	Reserved bytes
ICMP	None	First 8 bytes
Udpprivate	None	First 1 byte
Udppublic	None	First 1 byte
jitter	None	First 68 bytes
jitter	G.711 A-Law	First 16 bytes
jitter	G.711 muHmm-Law	First 16 bytes
jitter	G.729 A-Law	First 16 bytes

Examples

Configure a packet padding string **12 ab cd**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] datafill 12 ab cd
```

datasize

Syntax

datasize *size*

undo datasize

View

remote-ping test group view

Parameters

size: Size of a test packet in bytes. The value range varies with the test types.

Table 1-2 Value range of the remote-ping test packets

Test Type	Code	Range	Default value
Jitter	None	68-8100	68
Jitter	G.711 A-Law	16-1500	172
Jitter	G.711 U-Law	16-1500	172
Jitter	G.729 A-Law	16-1500	32
ICMP	None	4-8100	56

Test Type	Code	Range	Default value
UDP	None	4-8100	100
Other	None	4-8100	0

Description

Use the **datasize** command to configure the size of a test packet in a test.

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

The configuration of packet size is only supported by ICMP, UDP and jitter tests.

Examples

Set the size of ICMP test packets to 50 bytes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] datasize 50
```

description

Syntax

description *string*

undo description

View

remote-ping test group view

Parameters

string: Brief description about a test operation. By default, no description is configured.

Description

Use the **description** command to briefly describe a test operation.

Use the **undo description** command to delete the configured description.

Examples

Describe a test group as “icmp-test”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] description icmp-test
```

destination-ip

Syntax

destination-ip *ip-address*

undo destination-ip

View

remote-ping test group view

Parameters

ip-address: Destination IP address of a remote-ping test.

Description

Use the **destination-ip** command to configure a destination IP address of an remote-ping test.

Use the **undo destination-ip** command to remove the configured destination IP address.

By default, no destination IP address is configured for an remote-ping test.

Related commands: **destination-port**.

Note

The destination address can be an IP address or a host name in HTTP test, while in other types of tests, it must be an IP address.

Examples

Set the destination IP address of an ICMP test to 169.254.10.3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] destination-ip 169.254.10.3
```

destination-port

Syntax

destination-port *port-number*

undo destination-port

View

remote-ping test group view

Parameters

port-number: Destination port number for an remote-ping test, in the range of 1 to 50000.

Description

Use the **destination-port** command to configure a destination port number for an remote-ping test.

Use the **undo destination-port** command to remove the configured destination port number.

By default, no destination port number is configured for a test.

Related commands: **destination-ip**.

Note

- The **destination-port** command has effect on jitter, TCP-Private, and UDP-Private tests only.
- It is not recommended to perform a TCP, UDP, or jitter test on a well-known port (ports with a number ranging from 1 to 1023) . Otherwise, the remote-ping test will fail or the corresponding service of the well-known port will become unavailable.

Examples

Set the destination port number for a tcpprivate test to 9000.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator tcp
[Sysname-remote-ping-administrator-tcp] test-type tcpprivate
[Sysname-remote-ping-administrator-tcp] destination-port 9000
```

display remote-ping

Syntax

display remote-ping { **results** | **history** | **jitter** } [*administrator-name operation-tag*]

View

Any view

Parameters

results: Displays results of the last test.

history: Displays the history records of tests.

jitter: Displays the jitter test information.

administrator-name: Name of the administrator who created the remote-ping test operation, a string of 1 to 32 characters.

operation-tag: Operation tag, a string of 1 to 32 characters.

Description

Use the **display remote-ping** command to display the result of the last remote-ping test or the history of remote-ping tests.

Without *administrator-name test-operation-tag* specified, the command displays the results of all test groups; without *administrator-name test-operation-tag* specified, the command displays the results of the specified test group.

Related commands: **test-enable**.

Examples

Display the test results of the test group with administrator name **administrator**, and operation tag **icmp**.

```
<Sysname> display remote-ping results administrator icmp
  remote-ping entry(admin administrator, tag icmp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10             Receive response times: 10
      Min/Max/Average Round Trip Time: 1/2/1
      Square-Sum of Round Trip Time: 13
      Last succeeded test time: 2004-11-25 16:28:55.0
  Extend result:
      SD Maximal delay: 0                  DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
```

Table 1-3 Description on the fields of the **display remote-ping result** command

Field	Description
Destination ip address	Destination IP address
Send operation times	Number of probes made
Receive response times	Number of received response packets
Min/Max/Average Round Trip Time	Minimum/maximum/average roundtrip time, in milliseconds
Square-Sum of Round Trip Time	Square sum of roundtrip time
Last succeeded test time	Completion time of the last successful test
SD Maximal delay	Maximum delay from the source to the destination
DS Maximal delay	Maximum delay from the destination to the source
Packet lost in test	Average packet loss ratio
Disconnect operation number	Number of times the test was disconnected by the remote end
System busy operation number	Number of times the test failed because the system was busy
Operation sequence errors	Number of out-of-sequence packets received
Other operation errors	Number of other errors
Operation timeout number	Number of time-out occurrences in a test
Connection fail number	Number of failures to connect with the remote end
Drop operation number	Number of system resource allocation failures

Display the history records of remote-ping tests.

```
<Sysname> display remote-ping history administrator icmp
  remote-ping entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LastRC      Time
        1            1         1           0    2004-11-25 16:28:55.0
        2            1         1           0    2004-11-25 16:28:55.0
        3            1         1           0    2004-11-25 16:28:55.0
        4            1         1           0    2004-11-25 16:28:55.0
        5            1         1           0    2004-11-25 16:28:55.0
        6            2         1           0    2004-11-25 16:28:55.0
        7            1         1           0    2004-11-25 16:28:55.0
        8            1         1           0    2004-11-25 16:28:55.0
        9            1         1           0    2004-11-25 16:28:55.9
       10            1         1           0    2004-11-25 16:28:55.9
```

Table 1-4 Description on the fields of the **display remote-ping history** command

Field	Description
Response	Roundtrip time in the case of a successful test, timeout time in the case of test timeout, or 0 in the case of a test failure (in milliseconds)
Status	Test result values, including: 1: responseReceived: Response received 2: unknown: Unknown error. 3: internalError: System internal error 4: requestTimeOut: Request timed out 5: unknownDestinationAddress: Unknown destination address 6: noRouteToTarget: Destination unreachable 7: interfaceInactiveToTarget: Interface to destination address inactive 8: arpFailure: ARP operation failed. 9: maxConcurrentLimitReached: Maximum limit of concurrent accesses reached 10: unableToResolveDnsName: Unable to resolve DNS domain name 11: invalidHostAddress: Invalid host address
LastRC	Response code in the last ICMP response packet received. (The device does not support this field at present, so this field is always displayed as 0.)
Time	Test completion time

Display the test results of the test group with administrator name **administrator**, and operation tag **http**.

```
[Sysname-remote-ping-administrator-http] display remote-ping results administrator http
  remote-ping entry(admin dns, tag 1) test result:
      Destination ip address:192.168.0.73
      Send operation times: 1              Receive response times: 1
      Min/Max/Average Round Trip Time: 27/27/27
```

```
    Square-Sum of Round Trip Time: 729
    Last succeeded test time: 2000-4-2 3:45:36.8
Extend result:
    SD Maximal delay: 0                  DS Maximal delay: 0
    Packet lost in test: 0%
    Disconnect operation number: 0       Operation timeout number: 0
    System busy operation number: 0      Connection fail number: 0
    Operation sequence errors: 0         Drop operation number: 0
    Other operation errors: 0
  Http result:
    DNS Resolve Time: 0                  HTTP Operation Time: 7
    DNS Resolve Min Time: 0              HTTP Test Total Time: 27
    DNS Resolve Max Time: 0          HTTP Transmission Successful Times: 1
    DNS Resolve Failed Times: 0          HTTP Transmission Failed Times: 0
    DNS Resolve Timeout Times: 0        HTTP Transmission Timeout Times: 0
    TCP Connect Time: 20                 HTTP Operation Min Time: 7
    TCP Connect Min Time: 20             HTTP Operation Max Time: 7
    TCP Connect Max Time: 20
    TCP Connect Timeout Times: 0
```

Table 1-5 Description on the fields of the **display remote-ping result** command

Field	Description
DNS Resolve Time	Time used for a DNS resolution
HTTP Operation Time	Total time used to establish an HTTP connection
DNS Resolve Min Time	Minimal time used for a DNS resolution
HTTP Test Total Time	Total time used for an HTTP test
DNS Resolve Max Time	Maximum time used for a DNS resolution
HTTP Transmission Successful Times	Number of successful HTTP transmissions
DNS Resolve Failed Times	Number of failed DNS resolutions
HTTP Transmission Failed Times	Number of failed HTTP transmissions
DNS Resolve Timeout Times	DNS resolution timeout times
HTTP Transmission Timeout Times	HTTP transmission timeout times
TCP Connect Time	Total time used to establish a TCP connection
HTTP Operation Min Time	Minimum time used to establish an HTTP connection
TCP Connect Min Time	Minimum time used to establish a TCP connection
HTTP Operation Max Time	Maximum time used to establish an HTTP connection
TCP Connect Max Time	Maximum time used to establish a TCP connection
TCP Connect Timeout Times	TCP connection timeout times

Display the test results of the test group with administrator name **administrator**, and operation tag **Jitter**.

```
<Sysname> display remote-ping results administrator Jitter
remote-ping entry(admin administrator, tag Jitter) test result:
      Destination ip address:10.2.2.2
      Send operation times: 100             Receive response times: 100
      Min/Max/Average Round Trip Time: 9/21/13
      Square-Sum of Round Trip Time: 18623
      Last succeeded test time: 2000-4-2 8:14:58.2
  Extend result:
      SD Maximal delay: 10                  DS Maximal delay: 10
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Jitter result:
      RTT Number:100
      Min Positive SD:1                   Min Positive DS:1
      Max Positive SD:6                   Max Positive DS:8
      Positive SD Number:38               Positive DS Number:25
      Positive SD Sum:85                  Positive DS Sum:42
      Positive SD average:2               Positive DS average:1
      Positive SD Square Sum:267          Positive DS Square Sum:162
      Min Negative SD:1                   Min Negative DS:1
      Max Negative SD:6                   Max Negative DS:8
      Negative SD Number:30               Negative DS Number:24
      Negative SD Sum:64                  Negative DS Sum: 41
      Negative SD average:2               Negative DS average:1
      Negative SD Square Sum:200          Negative DS Square Sum:161
      SD lost packets number:0            DS lost packet number:0
      Unkown result lost packet number:0
```

Table 1-6 Description on the fields of the **display remote-ping result** command

Field	Description
RTT Number	Number of received response packets
Min Positive SD	Minimum positive jitter delay from the source to the destination
Min Positive DS	Minimum positive jitter delay from the destination to the source
Max Positive SD	Maximum positive jitter delay from the source to the destination
Max Positive DS	Maximum positive jitter delay from the destination to the source
Positive SD Number	Number of positive jitter delays from the source to the destination

Field	Description
Positive DS Number	Number of positive jitter delays from the destination to the source
Positive SD Sum	Sum of positive jitter delays from the source to the destination
Positive DS Sum	Sum of positive jitter delays from the destination to the source
Positive SD average	Average of positive jitter delays from the source to the destination
Positive DS average	Average of positive jitter delays from the destination to the source
Positive SD Square Sum	Sum of the square of positive jitter delays from the source to the destination
Positive DS Square Sum	Sum of the square of positive jitter delays from the destination to the source
Min Negative SD	Minimum absolute value of negative jitter delays from the source to the destination
Min Negative DS	Minimum absolute value of negative jitter delays from the destination to the source
Max Negative SD	Maximum absolute value of negative jitter delays from the source to the destination
Max Negative DS	Maximum absolute value of negative jitter delays from the destination to the source
Negative SD Number	Number of negative jitter delays from the source to the destination
Negative DS Number	Number of negative jitter delays from the destination to the source
Negative SD Sum	Sum of absolute values of negative jitter delays from the source to the destination
Negative DS Sum	Sum of absolute values of negative jitter delays from the destination to the source
Negative SD average	Average of negative jitter delays from the source to the destination
Negative DS average	Average of negative jitter delays from the destination to the source
Negative SD Square Sum	Sum of the square of negative jitter delays from the source to the destination
Negative DS Square Sum	Sum of the square of negative jitter delays from the destination to the source
SD lost packets number	Number of lost packets from the source to the destination
DS lost packet number	Number of lost packets from the destination to the source
Unknown result lost packet number	Number of lost packets for unknown reasons

Display the test results of the test group with administrator name **administrator**, and operation tag **dns**.

```
<Sysname> display remote-ping results administrator dns
remote-ping entry(admin administrator, tag dns) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 6/10/8
      Square-Sum of Round Trip Time: 756
      Last succeeded test time: 2006-11-28 11:50:40.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Dns result:
      DNS Resolve Current Time: 10         DNS Resolve Min Time: 6
      DNS Resolve Times: 10                DNS Resolve Max Time: 10
      DNS Resolve Timeout Times: 0         DNS Resolve Failed Times: 0
```

Table 1-7 Description on the fields of the **display remote-ping result** command

Field	Description
DNS Resolve Current Time	Time used for the current DNS resolution
DNS Resolve Min Time	Minimum time used for a DNS resolution
DNS Resolve Times	Number of DNS resolutions
DNS Resolve Max Time	Maximum time used for a DNS resolution
DNS Resolve Timeout Times	DNS resolution timeout times
DNS Resolve Failed Times	Number of failed DNS resolutions

Note

The description on a specific field is available for the test results of all types of tests, so that not the description on the output information of all types of tests is provided here.

display remote-ping statistics

Syntax

display remote-ping statistics [*administrator-name operation-tag*]

View

Any view

Parameters

administrator-name: Name of the administrator creating the test.

operation-tag: Test operation tag.

Description

Use the **display remote-ping statistics** command to display test statistics.

After a test begins, if all the probes in the first test have not been finished, when you use the command to view statistics, all statistics results will be 0.

Examples

Display the statistics information for admin jitter test group, the test type of which is jitter.

```
<Sysname> display remote-ping statistics admin jitter
remote-ping entry(admin admin, tag jitter) statistics record:
   No. :        1
   Destination ip address:   169.254.10.3
   StartTime:      2000/1 /2  3 :12:44
   LifeTime:       21
   Send operation times:    0             Receive response times:   0
   Max Round Trip Time:     0           Min Round Trip Time:      0
   Sum Round Trip Time:     0           Average Round Trip Time:  0
   Square-Sum of Round Trip Time: 0       Packet lost in test:      0%
   Disconnect operation number: 0         Operation timeout number: 0
   System busy operation number:0         Connection fail number:   0
   Operation sequence errors:   0         Drop operation number:    0
   Other operation errors:      0
    Jitter result:
      Min Positive SD:0                   Min Positive DS:0
      Max Positive SD:0                   Max Positive DS:0
      Positive SD Number:0                Positive DS Number:0
      Positive SD Sum:0                   Positive DS Sum:0
      Positive SD average:0               Positive DS average:0
      Positive SD Square Sum:0            Positive DS Square Sum:0
      Min Negative SD:0                   Min Negative DS:0
      Max Negative SD:0                   Max Negative DS:0
      Negative SD Number:0                Negative DS Number:0
      Negative SD Sum:0                   Negative DS Sum: 0
      Negative SD average:0               Negative DS average:0
      Negative SD Square Sum:0            Negative DS Square Sum:0
      SD lost packets number:0            DS lost packet number:0
      SD packet lost in test:0%           DS packet lost in test:0%
      Unknown result lost packet number:0
```

Table 1-8 Description on fields in the output of the **display remote-ping statistic** command

Field	Description
Start time	The time when a test starts

Field	Description
Lifetime	The time that a test lasts
Send operation times	The number of the sent test packets.
Receive response times	The number of successful test attempts
Min/Max/Average Round Trip Time	Roundtrip time in its minimum, maximum, and average
Square-Sum of Round Trip Time	The square sum of roundtrip time
Packet lost in test	The number of lost packets in a test
Disconnect operation number	The number of forcible disconnections performed by the opposite end
Operation timeout number	The number of timeout in a test
System busy operation number	The number of test failures due to busy system
Connection fail number	The number of connection failures to the opposite end
Operation sequence errors	The number of received disordered packets
Drop operation number	The number of failures in allocating system resource
Other operation errors	The number of other operation errors
Min Positive SD (DS)	The jitter value from source to destination (destination to source) is the minimum of positive value
Max Positive SD (DS)	The jitter value from source to destination (destination to source) is the maximum of positive value
Positive SD (DS) number/sum/average/square sum	The jitter value from source to destination (destination to source) is the number/sum/average/square sum of positive jitter values
Min Negative SD (DS)	The jitter value from source to destination (destination to source) is the minimum of negative value
Max Negative SD (DS)	The jitter value from source to destination (destination to source) is the maximum of negative value
Negative SD (DS) number/sum/average/square sum	The jitter value from source to destination (destination to source) is the number/sum/average/square sum of negative jitter values
SD (DS) lost packets number	The number of the lost packets from source to destination (destination to source) This value has nothing to do with NTP synchronization.
SD (DS) packet lost in test	Packet loss ratio from source to destination (destination to source) in one test This value has nothing to do with NTP synchronization.

Field	Description
Unknown result lost packet number	The number of the lost packets for unknown reason

dns-server

Syntax

dns-server *ip-address*

undo dns-server

View

remote-ping test group view

Parameters

ip-address: IP address to be assigned to a domain name server (DNS).

Description

Use the **dns-server** command to configure the IP address of a DNS server.

Use the **undo dns-server** command to remove the IP address of a DNS server.

By default, no DNS server IP address is configured.

Note

- This command applies to DNS and HTTP tests only.
- For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test

Examples

Set the IP address of the DNS server to 169.254.10.5.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator dns
[Sysname-remote-ping-administrator-dns] test-type dns
[Sysname-remote-ping-administrator-dns] dns-server 169.254.10.5
```

dns resolve-target

Syntax

dns resolve-target *domain-name*

undo dns resolve-target

View

remote-ping test group view

Parameters

domain-name: Domain name to be resolved, in the range of 1 to 60 characters.

Description

Use the **dns resolve-target** command to configure a domain name to be resolved.

Use the **undo resolve-target** command to remove a domain name to be resolved.

By default, no dns resolve-target information is configured.

Note

This command applies to DNS tests only.

Examples

Configure the domain name to be resolved as **www.test.com**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator dns
[Sysname-remote-ping-administrator-dns] test-type dns
[Sysname-remote-ping-administrator-dns] dns resolve-target www.test.com
```

filename

Syntax

filename *file-name*

undo filename

View

remote-ping test group view

Parameters

file-name: Name of the file to be downloaded/uploaded in FTP tests, a string of 1 to 230 characters.

Description

Use the **filename** command to specify a file to be downloaded/uploaded in FTP tests.

Use the **undo filename** command to remove the configured file name.

By default, no file name is configured for FTP tests.

Related commands: **username**, **password**, **ftp-operation**.

Note

The **filename** command applies to FTP tests only.

Examples

Specify to transmit **config.txt** between remote-ping client and FTP server in an FTP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
[Sysname-remote-ping-administrator-ftp] filename config.txt
```

filesize

Syntax

filesize *size*

undo filesize

View

remote-ping test group view

Parameters

size: File size, in the range 1 to 10000 Kbytes.

Description

Use the **filesize** command to configure the size of the file to be uploaded in an FTP test.

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

By default, the file size is 1000 Kbytes.

Related commands: **username**, **password**, **ftp-operation**.

Note

This command applies only to the PUT operation of an FTP test.

Examples

Configure the file to be uploaded in an FTP test as 2000 KByte.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
```

```
[Sysname-remote-ping-administrator-ftp] ftp-operation put
[Sysname-remote-ping-administrator-ftp] filesize 2000
```

frequency

Syntax

frequency *interval*

undo frequency

View

remote-ping test group view

Parameters

interval: Automatic test interval in seconds. It ranges from 0 to 65,535.

Description

Use the **frequency** command to configure the time interval of performing automatic tests.

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

If *interval* is configured greater than 0, the system performs automatic tests at this interval.

interval defaults to 0, which means no automatic test is performed by default.

Related commands: **count**.

 **Note**

- The **frequency** command does not apply to DHCP tests.
- The **frequency** command supports fabric only when the test type of this test group is ICMP. With fabric enabled, you are allowed to configure the **frequency** command and use the **display** command to check your configuration, but unless the test type is ICMP, your configuration does not take effect until fabric is disabled.

Examples

Set the automatic test interval to 10 seconds in an ICMP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] destination-ip 169.254.10.3
[Sysname-remote-ping-administrator-icmp] frequency 10
```

ftp-operation

Syntax

ftp-operation { **get** | **put** }

View

remote-ping test group view

Parameters

get: Specifies the test operation as download from the FTP server.

put: Specifies the test operation as upload to the FTP server.

Description

Use the **ftp-operation** command to configure the FTP operation mode, which can be **get** and **put**.

By default, the FTP operation mode is **get**.

Related commands: **username**, **password**.

Note

The **ftp-operation** command applies to FTP tests only.

Examples

Set the FTP operation mode to **put** in an FTP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
[Sysname-remote-ping-administrator-ftp] ftp-operation put
```

history keep-time

Syntax

history keep-time *keep-time*

undo history keep-time

View

remote-ping test group view

Parameters

keep-time: Retaining time of the history record for a test group, which is in the range 1 to 1440 in minutes and defaults to 120 minutes.

Description

Use the **history keep-time** command to configure the retaining time of the history record for a test group.

Use the **undo history keep-time** command to restore the default.

Examples

Configure the retaining time of the history record for a test group to 240 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] history keep-time 240
```

history-record enable

Syntax

history-record enable

undo history-record enable

View

remote-ping test group view

Parameters

None

Description

Use the **history-record enable** command to enable history record.

Use the **undo history-record enable** command to disable history record.

By default, history record is disabled. You should configure to save history record as needed.

- If you need to save history record, enable it.
- If you disable the history record after enabling it, the saved history record will be deleted and the maximum number of the history record for you to save will not be changed.
- If you do not need to save history record, disable it. At this time you can also configure the number of the history record to be saved, but the history record will not be saved.

Use the **display remote-ping history** command to view the history record.

Examples

Enable history record saving.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] history-record enable
```

history-records

Syntax

history-records *number*

undo history-records

View

remote-ping test group view

Parameters

Number: Maximum number of history records that can be saved in a test group, in the range of 0 to 50, and 50 by default.

Description

Use the **history-records** command to set the maximum number of history records that can be saved in a test group.

Use the **undo history-records** to restore the default.

By default, up to 50 records can be saved in a test group.

Examples

Set the maximum number of history records that can be saved to 10.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] history-records 10
```

http-operation

Syntax

http-operation { **get** | **post** }

View

remote-ping test group view

Parameters

get: Specifies the test operation to be download from the HTTP server.

post: Specifies the test operation to be uploaded to the HTTP server.

Description

Use the **http-operation** command to configure the HTTP operation mode.

By default, the HTTP operation mode is **get**.

Note

The **http-operation** command applies to HTTP tests only.

Examples

Set the HTTP operation mode to **post** in an HTTP test.

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

```
[Sysname] remote-ping administrator http
[Sysname-remote-ping-administrator-http] test-type http
[Sysname-remote-ping-administrator-http] http-operation post
```

http-string

Syntax

http-string *string version*

undo http-string

View

remote-ping test group view

Parameters

string: HTTP operation string used to specify the webpage to be accessed. It can consist of 1 to 230 characters.

version: HTTP version, a string of 1 to 12 characters. At present, this argument can be HTTP/1.0 or HTTP/1.1, where HTTP must be capitalized.

Description

Use the **http-string** command to configure the HTTP operation string and HTTP version.

Use the **undo http-string** command to remove the configured HTTP operation string and version.

By default, no HTTP operation string and HTTP version are configured.

Note that the **http-string** command applies to HTTP tests only.

Related commands: **http-operation**.

Examples

Configure the webpage to be accessed by an HTTP test as **/index.htm** and the HTTP version as **HTTP/1.0**.

```
<Sysname> system-view
[Sysname] remote-ping administrator http
[Sysname-remote-ping-administrator-http] test-type http
[Sysname-remote-ping-administrator-http] http-string /index.htm HTTP/1.0
```

remote-ping

Syntax

remote-ping *administrator-name operation-tag*

undo remote-ping *administrator-name operation-tag*

View

System view

Parameters

administrator-name: Name of the administrator to create a remote-ping test group, a string of 1 to 32 characters.

operation-tag: Operation tag, a string of 1 to 32 characters.

Description

Use the **remote-ping** command to create an remote-ping test group and enter remote-ping test group view. If the specified remote-ping test group already exists, this command leads you to remote-ping test group view directly.

Use the **undo remote-ping** command to delete an remote-ping test group.

Examples

Create an remote-ping test group of which the administrator name is **administrator** and operation tag is **icmp**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp]
```

remote-ping-agent clear

Syntax

remote-ping-agent clear

View

System view

Parameters

None

Description

Use the **remote-ping-agent clear** command to clear all agents on the remote-ping client.

Examples

Clear all currently configured agents.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-agent clear
```

remote-ping-agent enable

Syntax

remote-ping-agent enable

undo remote-ping-agent enable

View

System view

Parameters

None

Description

Use the **remote-ping-agent enable** command to enable the remote-ping client function.

Use the **undo remote-ping-agent enable** command to disable the remote-ping client function.

By default, the remote-ping client function is disabled.

You can perform tests only after you enable the remote-ping client function.

Related commands: **remote-ping-server enable**.

Examples

Enable remote-ping client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-agent enable
```

remote-ping-agent max-requests

Syntax

remote-ping-agent max-requests *max-number*

undo **remote-ping-agent max-requests**

View

System view

Parameters

max-number: Maximum number of concurrent tests, in the range of 1 to 5.

Description

Use the **remote-ping-agent max-requests** command to set the allowed maximum number of concurrent tests.

Use the **undo remote-ping-agent max-requests** command to restore the default maximum number of concurrent tests, that is, five tests.

 **Note**

This command applies to DHCP test only.

Examples

Set the maximum number of concurrent tests to 4.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-agent max-requests 4
```

jitter-interval

Syntax

jitter-interval *interval*

undo jitter-interval

View

remote-ping test group view

Parameters

interval: Interval in milliseconds between jitter test packets. The value is in the range of 10 to 1000.

Description

Use the **jitter-interval** command to configure the interval between sending jitter test packets.

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

By default, the interval between sending jitter test packets is 20 milliseconds.

Related commands: **jitter-packetnum**.

Note

The **jitter-interval** command applies to jitter tests only.

Examples

Set the interval between sending jitter test packets to 30 milliseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator jitter
[Sysname-remote-ping-administrator-jitter] test-type jitter
[Sysname-remote-ping-administrator-jitter] jitter-interval 30
```

jitter-packetnum

Syntax

jitter-packetnum *number*

undo jitter-packetnum

View

remote-ping test group view

Parameters

number: Number of packets to be transmitted in one probe for a jitter test, in the range of 10 to 1000.

Description

Use the **jitter-packetnum** command to configure the number of packets to be sent in one probe for a jitter test.

Use the **undo jitter-packetnum** command to restore the default.

By default, 10 packets are sent in a probe for a jitter test.

Related commands: **jitter-interval**.

Note

This command applies to jitter tests only.

Examples

Configure to send 30 packets in a probe for a jitter test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator jitter
[Sysname-remote-ping-administrator-jitter] test-type jitter
[Sysname-remote-ping-administrator-jitter] jitter-packetnum 30
```

password

Syntax

password *password*

undo password

View

remote-ping test group view

Parameters

password: Password for logging in to an FTP server, a string of 1 to 32 characters.

Description

Use the **password** command to configure a password for logging in to the FTP server.

Use the **undo password** command to remove the configured password.

By default, the password for logging in to the FTP server is not configured.

Related commands: **username**, **ftp-operation**.

Note

- To perform an FTP test successfully, the configured password must be consistent with the FTP user password configured on the server.
- This command applies to FTP tests only.

Examples

Set the password for logging into the FTP server as **remote-ping** in an FTP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
[Sysname-remote-ping-administrator-ftp] password remote-ping
```

probe-failtimes

Syntax

probe-failtimes *times*

undo probe-failtimes

View

remote-ping test group view

Parameters

times: Number of consecutive failed probes, in the range of 1 to 15.

Description

Use the **probe-failtimes** command to configure the number of consecutive times the probe fails before the switch sends out a trap message.

Use the **undo probe-failtimes** command to restore the default.

By default, the switch sends a trap about probe failure each time when a probe fails.

Examples

Configure the switch to send a trap after the probe in an ICMP test fails for three consecutive times.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] probe-failtimes 3
```

send-trap

Syntax

send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** }* }

undo send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** }* }

View

remote-ping test group view

Parameters

probefailure: Sends a trap when a probe fails.

testcomplete: Sends a trap after a test is finished.

testfailure: Sends a trap when a test fails.

all: Sends a trap when any of the above-mentioned scenarios occurs.

Description

Use the **send-trap** command to enable debugging for a trap.

Use the **undo send-trap** command to disable debugging for a trap.

By default, no trap is output.

Examples

Send a trap message after an ICMP test is finished.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] send-trap testcomplete
```

sendpacket passroute

Syntax

sendpacket passroute

undo sendpacket passroute

View

remote-ping test group view

Parameters

None

Description

Use the **sendpacket passroute** command to enable routing table bypass.

Use the **undo sendpacket passroute** command to disable routing table bypass.

By default, routing table bypass is disabled.

With routing table bypass, a remote host can bypass the normal routing tables and send ICMP packets directly to a host on an attached network. If the host is not on a directly connected network, an error is returned. You can use this function when pinging a local host on an interface that has no route defined.

Examples

Bypass routing table when sending ICMP packets.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] sendpacket passroute
```

source-interface

Syntax

source-interface *interface-type interface-number*

undo source-interface

View

remote-ping test group view

Parameters

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

Description

For ICMP tests, use the **source-interface** command to specify a source interface for sending ICMP requests. The corresponding IP address of the specified interface is used as the source IP address of ICMP requests. For DHCP tests, use the **source-interface** command to specify an interface for DHCP probes.

For ICMP tests, use the **undo source-interface** command to remove the specified source interface, and its corresponding IP address is no longer used as the source IP address of ICMP requests. For DHCP tests, use the **undo source-interface** command to remove the specified interface for DHCP probes.

By default, no source interface is specified for ICMP tests and no interface is configured for DHCP probes.

Note

- For DHCP tests, this command is required. For ICMP tests, this command is optional. This command does not apply to other tests.
- For ICMP tests, if a source IP address has been configured with the **source-ip** command, the **source-interface** command cannot change the configured IP address.
- For an ICMP test, if a source interface has been configured with the **source-interface** command, the test destination address should be configured as the address of the device directly connected to the interface. Otherwise, the test will fail.
- The interface to be specified in this command can be only a VLAN interface.
- The interface to be specified must be Up; otherwise the test will fail.

Examples

Configure the source interface that sends test packets in DHCP tests as VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator dhcp
[Sysname-remote-ping-administrator-dhcp] test-type dhcp
[Sysname-remote-ping-administrator-dhcp] source-interface Vlan-interface 1
```

source-ip

Syntax

source-ip *ip-address*

undo source-ip

View

remote-ping test group view

Parameters

ip-address: Source IP address for a test.

Description

Use the **source-ip** command to configure the source IP address for the test.

Use the **undo source-ip** command to remove the configured source IP address.

By default, the IP address of the interface that sends test packets serves as the source IP address.

Note

- For FTP tests, this command is required. This command does not apply to DHCP tests. For other tests, this command is optional.
- The specified source IP address by this command cannot be of an interface on a remote device, and the interface must be Up; otherwise the test will fail.

Examples

Configure the source IP address as 169.254.10.2 for this ICMP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] source-ip 169.254.10.2
```

source-port

Syntax

source-port *port-number*

undo source-port

View

remote-ping test group view

Parameters

port-number: Protocol source port number, in the range of 1 to 50000.

Description

Use the **source-port** command to configure the protocol source port number for the current test.

Use the **undo source-port** command to remove the configured source port number.

Note

This command does not apply to ICMP, DHCP, and DNS tests.

Examples

Configure the source port number as 8000 for the tcpprivate test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator tcpprivate
[Sysname-remote-ping-administrator-tcpprivate] test-type tcpprivate
```

```
[Sysname-remote-ping-administrator-tcpprivate] source-port 8000
```

statistics

Syntax

statistics { **interval** *interval* **| max-group** *number* }

undo statistics { **interval | max-group** }

View

remote-ping test group view

Parameters

interval: Statistics interval, in the range 1 to 1440, in minutes, and defaults to 60 minutes.

number: Number of groups of statistics information, in the range 1 to 100 and defaults to 2.

Description

Use the **statistics** command to configure the statistics interval and the maximum number of the groups of the retained statistics information according to the configuration.

Use the **undo statistics** command to remove your configuration and restore the default.

By default, the statistics interval for a test is once every 60 minutes and up to two groups of statistics information can be retained.

Delete all statistics information when internet parameter changes.

Examples

Set the statistics interval to 120 minutes and the maximum number of statistics groups to three.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] statistic interval 120
[Sysname-remote-ping-administrator-icmp] statistic max-group 3
```

statistics keep-time

Syntax

statistics keep-time *keep-time*

undo statistics keep-time

View

remote-ping test group view

Parameters

keep-time: Retaining time of the test statistics, which is in the range 1 to 1440 in minutes and defaults to 120 minutes.

Description

Use the **statistics keep-time** command to configure the retaining time of the test statistics.

Use the **undo statistics keep-time** command to remove your configuration and restore the default.

Examples

Configure the retaining time of the test statistics to 180 minutes.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] statistics keep-time 180
```

test-time begin

Syntax

test-time begin { *hh*:*mm* :*ss* [*yyyy/mm/dd*] | **now** } **lifetime** *lifetime*

undo test-time

View

remote-ping test group view

Parameters

hh:mm:ss: Test start time.

yyyy/mm/dd: Test start time, *yyyy* is the year in the range 2000 to 2099, *mm* is the month in the range 1 to 12 and *dd* is the date in the range 1 to 31.

now: Specifies a test that starts from now.

lifetime: Lasting time of a test, in the range 1 to 2147483647 in seconds.

Description

Use the **test-time begin** command to configure the start time and the lasting time of a test.

Use the **undo test-time** command to stop the test and remove the configuration.

- When the test is not performed, the configuration information you input is saved, including test start time and lasting time.
- If you set a start time earlier than the current system time or the test lasting time you configured is 0, the test will not be performed.
- When a test is being performed, you cannot perform any configuration; otherwise the system prompts error.
- After you configure this command, if the test-related parameters are not complete, the system prompts configuration error.
- The test starts until you execute the **test-time begin** command.
- If you set a start time earlier than the current system time, when you modify the current system time, the test will not be performed.
- If **lifetime** of the test group expires, the test will stop and when you modify the current system time, the test will not be performed.

Examples

Set the test to start from 14:03 and last 3600 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-time begin 14:03:00 lifetime 3600
```

test-type

Syntax

test-type *type* [**codec** *codec-value*]

View

remote-ping test group view

Parameters

type: Test type. It can be any of the following keywords:

- **dhcp**: Indicates a DHCP test.
- **dns**: Indicates a DNS test.
- **ftp**: Indicates an FTP test.
- **http**: Indicates an HTTP test.
- **icmp**: Indicates an ICMP test.
- **jitter**: Analyzes the delay change of UDP packet transmission.
- **snmpquery**: Indicates an SNMP test.
- **tcpprivate**: Indicates a TCP test on a specified (unknown) port.
- **tcppublic**: Indicates a TCP test on port 7.
- **udpprivate**: Indicates a UDP test on a specified (unknown) port.
- **udppublic**: Indicates a UDP test on port 7.

codec-value: Coding type for a voice test, which can be configured for a Jitter test and can be the following keywords:

- g711a: Specifies coding type to G.711 A-Law.
- g711u: Specifies coding type to G.711 muHmm-Law.
- g729a: Specifies coding type to G.729A-Law.

Description

Use the **test-type** command to configure the test type.

The default test type is **icmp**.

Note

If you modify the test type, the parameter configuration, test results and history records of the original test type will be cleared.

Examples

Configure the test type as an FTP test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
```

test-enable

Syntax

test-enable

undo test-enable

View

remote-ping test group view

Parameters

None

Description

Use the **test-enable** command to enable a remote-ping test.

Use the **undo test-enable** command to disable a remote-ping test.

Related commands: **display remote-ping**.

Note

The result of the remote-ping test cannot be displayed automatically, and you need to use the **display remote-ping** command to display the test result.

Examples

Perform a remote-ping test on an ICMP test group with the administrator name and operation tag being **administrator** and **icmp** respectively.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] destination-ip 169.254.10.3
[Sysname-remote-ping-administrator-icmp] test-enable
```

test-failtimes

Syntax

test-failtimes *times*

undo test-failtimes

View

remote-ping test group view

Parameters

times: Number of times of consecutive test failure, in the range of 1 to 15.

Description

Use the **test-failtimes** command to configure the number of consecutive times a remote-ping test fails before the switch sends out a trap message.

Use the **undo test-failtimes** command to restore the default.

By default, the switch sends a trap about test failure each time when a test fails.

Examples

Configure the switch to send out a trap message after an ICMP test fails for three consecutive times.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] test-failtimes 3
```

timeout

Syntax

timeout *time*

undo timeout

View

remote-ping test group view

Parameters

time: Timeout time for one probe, in the range of 1 to 60, in seconds.

Description

Use the **timeout** command to set the timeout time for a probe.

Use the **undo timeout** command to restore the default value.

The remote-ping client starts the probe timer after sending a test packet. If the remote-ping client receives no response before the timer expires, it considers that the current probe has timed out.

By default, the probe timeout time is 3 seconds.

Examples

Set the timeout time for one probe in an ICMP test to 10 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] timeout 10
```

tos

Syntax

tos value

undo tos

View

remote-ping test group view

Parameters

value: ToS value in a remote-ping test packet header, in the range of 0 to 255.

Description

Use the **tos** command to configure the ToS value in a remote-ping test packet header.

Use the **undo tos** command to remove the ToS value in a remote-ping test packet header.

By default, no ToS value is configured.

Note

This command does not apply to DHCP tests.

Examples

Set the ToS value in the header of an ICMP test packet to 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] test-type icmp
[Sysname-remote-ping-administrator-icmp] tos 1
```

ttl

Syntax

ttl number

undo ttl

View

remote-ping test group view

Parameters

number: Time to live (TTL) value or lifetime of remote-ping test packets. It is in the range 1 to 255 and defaults to 20.

Description

Use the **ttl** command to configure TTL of remote-ping test packets.

Use the **undo ttl** command to restore the default TTL of remote-ping test packets.

TTL is actually a hop count limit on how far a test packet can travel on a network. In a **ping** command, it is defined using the argument "-**h**".

Note

- This command applies to all types of tests except for DHCP and tracert tests.
- The **sendpacket passroute** command voids the **ttl** command.

Examples

Set the TTL of remote-ping ICMP test packets to 16.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator icmp
[Sysname-remote-ping-administrator-icmp] ttl 16
```

username

Syntax

username *name*

undo username

View

remote-ping test group view

Parameters

name: Username for logging in to an FTP server, a string of 1 to 32 characters.

Description

Use the **username** command to configure a username for logging in to the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username for logging in to the FTP server is configured.

Related commands: **password**, **ftp-operation**.

Note

- To perform an FTP test successfully, the configured username must be consistent with the username configured on the FTP server.
- This command applies to FTP tests only.

Examples

Configure the username for logging into the FTP server in an FTP test as **administrator**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping administrator ftp
[Sysname-remote-ping-administrator-ftp] test-type ftp
[Sysname-remote-ping-administrator-ftp] username administrator
```

remote-ping Server Commands

Note

- A remote-ping server is required for only jitter, TCP, and UDP tests.
- You are not recommended to configure remote-ping jitter/UDP/TCP servers on ports 1 through 1023 (well-known ports); otherwise, remote-ping probes may fail or the services corresponding to these ports may be unavailable.

remote-ping-server enable

Syntax

remote-ping-server enable

undo remote-ping-server enable

View

System view

Parameters

None

Description

Use the **remote-ping-server enable** command to enable the remote-ping server function.

Use the **undo remote-ping-server enable** command to disable the remote-ping server function.

By default, the remote-ping server function is disabled.

Related commands: **remote-ping-agent enable**, **remote-ping-server tcpconnect**, **remote-ping-server udpecho**.

Examples

Enable a remote-ping server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-server enable
```

remote-ping-server tcpconnect

Syntax

remote-ping-server tcpconnect *ip-address port-number*

undo remote-ping-server tcpconnect *ip-address port-number*

View

System view

Parameters

ip-address: IP address specified for a TCP listening service on the remote-ping server.

port-number: Port number specified for a TCP listening service on the remote-ping server. The value ranges from 1 to 50000. It is not recommended to use some special ports (that is, those used for fixed functions, such as port 1701). Otherwise, the remote-ping test may fail.

Description

Use the **remote-ping-server tcpconnect** command to create a TCP listening service on the remote-ping server.

Use the **undo remote-ping-server tcpconnect** command to remove the created TCP listening service.

When performing a TCP connection test on a specified port of a remote-ping client, you must create a TCP listening on the remote-ping server if the server is an switch; otherwise, the TCP test may fail.

Related commands: **remote-ping-server enable**.

Examples

Enable TCP listening, using 169.254.10.2 as the IP address and 9000 as the port number.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-server tcpconnect 169.254.10.2 9000
```

remote-ping-server udpecho

Syntax

remote-ping-server udpecho *ip-address port-number*

undo remote-ping-server udpecho *ip-address port-number*

View

System view

Parameters

ip-address: IP address from which a remote-ping server performs UDP listening.

port-number: Port from which a remote-ping server performs UDP listening. The value ranges from 1 to 49999. In is not recommended to use some special ports (that is, those used for fixed functions, such as port 1701). Otherwise, the remote-ping test may fail.

Description

Use the **remote-ping-server udpecho** command to enable UDP listening on a remote-ping server.

Use the **undo remote-ping-server udpecho** command to disable UDP listening.

When performing a jitter test or a UDP connection test on a specified port of a remote-ping client, you must enable UDP listening on the server if an Switch 4200G serves as a remote-ping server; otherwise, the test may fail.

Related commands: **remote-ping-server enable**.

Examples

Enable UDP listening, using 169.254.10.3 as the IP address and 9000 as the port number.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z
[Sysname] remote-ping-server udpecho 169.254.10.3 9000
```

Table of Contents

1 DNS Configuration Commands

DNS Configuration Commands

display dns domain

Syntax

display dns domain [**dynamic**]

View

Any view

Parameters

dynamic: Displays DNS suffixes dynamically assigned through DHCP or other protocols.

Description

Use the **display dns domain** command to display the DNS suffixes.

Related commands: **dns domain**.

Examples

Display DNS suffixes

```
<Sysname> display dns domain
No          Domain-name
0           aaa.com
```

Table 1-1 Description on the fields of the **display dns domain** command

Field	Description
No	Sequence number
Domain-name	DNS suffix

display dns dynamic-host

Syntax

display dns dynamic-host

View

Any view

Parameters

None

Description

Use the **display dns dynamic-host** command to display the information in the dynamic domain name cache.

Examples

Display the information in the dynamic domain name cache.

```
<Sysname> display dns dynamic-host
No Domain-name           --->    Ipaddress       TTL     Alias
1  lm.test.abc                   172.1.223.1     3564

No Domain-name           <---    Ipaddress       TTL     Alias
1  aaaa                          172.1.223.2     3594
```

Table 1-2 Description on the fields of the **display dns dynamic-host** command

Field	Description
No	Sequence number
Domain-name	Domain name
Ipaddress	IP address of the corresponding domain name
TTL	Time for which an entry is cached in seconds.
Alias	Alias for the domain name. There can be four aliases at most.
---> <---	DNS resolution has two types: Forward resolution: domain name--->IP address Reverse resolution: IP address--->domain name

display dns server

Syntax

display dns server [**dynamic**]

View

Any view

Parameters

dynamic: Displays the DNS Server information dynamically obtained through DHCP or other protocols.

Description

Use the **display dns server** command to display the DNS Server information.

Related commands: **dns server**.

Examples

Display the DNS Server information.

```
<Sysname> display dns server
 Type:
```

```
  D:Dynamic    S:Static

IPv4 DNS Servers :
Domain-server Type IP Address
     1        S    192.168.0.4

IPv6 DNS Servers :
```

Table 1-3 Description on the fields of the **display dns server** command

Field	Description
Type	Type of the DNS server. S indicates the DNS server is specified manually, while D indicates the DNS server information is obtained dynamically through DHCP or other protocols.
IPv4 DNS Servers	IPv4 DNS server
IPv6 DNS Servers	IPv6 DNS server
Domain-server	Number of the DNS server, which is assigned automatically by the system and starts from 1. Such numbering for IPv4 DNS servers is independent of that for IPv6 ones.

Note:

For details about IPv6 DNS, refer to *IPv6 Management Command*.

display ip host

Syntax

display ip host

View

Any view

Parameters

None

Description

Use the **display ip host** command to display mappings between host names and IP addresses in the static DNS database.

Examples

Display mappings between host names and IP addresses in the static DNS database.

```
<Sysname> display ip host
Host                          Age        Flags  Address
host.com                      0          static 192.168.0.38
```

Table 1-4 Description on the fields of the **display ip host** command

Field	Description
Host	Host name
Age	Time to live. 0 means that a static entry is never outdated. You can only manually remove the mappings between host names and IP addresses.
Flags	Indicates the type of mappings between host names and IP addresses, static or dynamic Static indicates static mapping between host names and IP addresses
Address	IP address of a host

dns domain

Syntax

dns domain *domain-name*

undo dns domain [*domain-name*]

View

System view

Parameters

domain-name: DNS suffix, a string of 1 to 60 characters which can be letters, numbers, hyphens (-), underscores (_), and dots (.).

Description

Use the **dns domain** command to configure a DNS suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use the **undo dns domain** command to delete the configured DNS suffix.

No DNS suffix is configured by default.

You can configure a maximum of 10 DNS suffixes. You must enter the DNS suffix before deleting it. Otherwise, all configured DNS suffixes are deleted.

Related commands: **display dns domain**.

Note

The DNS feature supported by S4200G series Ethernet switches should be used together with a DNS server. DNS implementations vary with DNS servers. For example, S4200G serial Ethernet switches support a domain name containing “_”, while a Windows 2000 Server may not be able to resolve the domain name.

Examples

Configure com as a DNS suffix.

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

dns resolve

Syntax

dns resolve

undo dns resolve

View

System view

Parameters

None

Description

Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

Examples

Enable dynamic domain name resolution.

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

dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

View

System view

Parameters

ip-address: IP address of the DNS Server.

Description

Use the **dns server** command to configure an IP address for the DNS Server.

Use the **undo dns server** to remove the IP address of the DNS server.

No IP address is configured for the DNS server by default.

You can configure a maximum of 6 DNS servers, including those with IPv6 addresses.

Related commands: **display dns server**.

Examples

Configure 172.16.1.1 for a DNS Server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dns server 172.16.1.1
```

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Parameters

hostname: Host name, a string of 1 to 20 characters which can be letters, numbers, hyphens (-), or dots (.). The host name must include at least one letter.

ip-address: IP address of the specified host, in dotted decimal notation.

Description

Use the **ip host** command to create a mapping between host name and IP address in the static DNS database.

Use the **undo ip host** command to remove the mapping.

No mappings are created by default.

Each host name can correspond to only one IP address. When IP addresses are configured for the same host for multiple times, only the IP address configured last time is valid.

Related commands: **display ip host**.

Examples

Configure IP address 10.110.0.1 for host aaa.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ip host aaa 10.110.0.1
```

nslookup type

Syntax

nslookup type { **ptr** *ip-address* | **a** *domain-name* }

View

Any view

Parameters

ptr *ip-address*: Displays the corresponding domain name for an IP address.

a *domain-name*: Displays the corresponding IP address for a DNS domain name. A domain name is a string of up to 30 characters. Automatic domain name addition is supported.

Description

Use the **nslookup type** command to display DNS resolution result, namely, the domain name for a specified IP address or IP address for a specified domain name.

Examples

Display the corresponding domain name for 192.168.3.2.

```
<Sysname> nslookup type ptr 192.168.3.2
Trying DNS server (10.72.66.36)
Name:    www.host.com
Address:  192.168.3.2
```

Display the corresponding IP address for www.host.com.

```
<Sysname> nslookup type a www.host.com
Trying DNS server  (10.72.66.36)
Name:    www.host.com
Address:  192.168.3.2
```

reset dns dynamic-host

Syntax

reset dns dynamic-host

View

User view

Parameters

None

Description

Use the **reset dns dynamic-host** command to clear information in the dynamic domain name cache.

Related commands: **display dns dynamic-host**.

Examples

Clear the information in the dynamic domain name cache.

```
<Sysname> reset dns dynamic-host
```

Table of Contents

1 Smart Link Configuration Commands

Smart Link Configuration Commands

display smart-link flush

Syntax

display smart-link flush

View

Any view

Parameters

None

Description

Use the **display smart-link flush** command to view the information about how the Smart Link device processes flush messages.

Examples

Display the information about how the Smart Link device processes flush messages.

```
<Sysname> display smart-link flush
Flush interface :GigabitEthernet1/0/1

 Count of flush packets received               : 1
 Time of last flush packet received            : 22:52:23 2006/04/01
 Source MAC of last flush packet received      : 000f-e20f-5566
 Device ID of last flush packet received       : 000f-e20f-5566
 Control VLAN ID of last flush packet received : 1
```

Table 1-1 Description on the fields of the **display smart-link flush** command

Field	Description
Flush interface	Interface that receives the latest legal flush message
Count of flush packets received	Total number of flush messages received
Time of last flush packet received	Time when the last legal flush message is received
Source MAC of last flush packet received	Source MAC address in the last legal flush message received
Device ID of last flush packet received	Bridge MAC address of the device from which the last legal flush message was received

Field	Description
Control VLAN ID of last flush packet received	Control VLAN ID in the last legal flush message received

Note

A legal flush message refers to the message whose control VLAN ID is consistent with the receiving control VLAN ID configured on the receiving port.

display smart-link group

Syntax

display smart-link group { *group-id* | **all** }

View

Any view

Parameters

group-id: Smart link group ID, in the range of 1 to 24.

all: Displays the information about all smart link groups.

Description

Use the **display smart-link group** command to display the information about the specific smart link group or all the smart link groups.

Examples

Display the information about smart link group 1.

```
<Sysname> display smart-link group 1
 Smart Link Group 1 information:
 Device ID: 000f-e212-3456              Control-VLAN ID: 1
 Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   1           16:37:20 2006/04/21
 AGG-1                     SLAVE   STANDBY  2           17:45:20 2006/04/21
```

Table 1-2 Description on the fields of the **display smart-link group** command

Field	Description
Member	Member of the smart link group
Role	Port role of a smart link group member: master or slave.
Status	Port status of a smart link group member when the link of this member port is up: active or standby.
Flush-count	Number of sent flush messages

Field	Description
Last-flush-time	Time when the last flush message is sent. If no flush message is sent, “NA” will be displayed.

flush enable control-vlan

Syntax

flush enable control-vlan *vlan-id*

undo flush enable

View

Smart link group view

Parameters

vlan-id: Control VLAN ID, in the range of 1 to 4,094.

Description

Use the **flush enable control-vlan** command to enable the function of sending flush messages in the specified control VLAN.

Use the **undo flush enable control-vlan** command to disable the function of sending flush messages to the specified control VLAN.

By default, no control VLAN is specified.

Examples

Configure to send flush messages within control VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] smart-link group 1
[Sysname-smlk-group1] flush enable control-vlan 1
```

link-aggregation group

Syntax

link-aggregation group *group-id* { **master** | **slave** }

undo link-aggregation group *group-id*

View

Smart link group view

Parameters

group-id: Link aggregation group ID, in the range of 1 to 50. Note that the specified link aggregation group can only be a static or manual one.

master: Specifies the specified link aggregation group as the master port of the smart link group.

slave: Specifies the specified link aggregation group as the slave port of the smart link group.

Description

Use the **link-aggregation group** command to assign a link aggregation group to the smart link group.

Use the **undo link-aggregation group** command to remove the specified link aggregation group from the smart link group.

 **Note**

Because Smart Link and STP cannot be enabled on an Ethernet port at the same time, you must make sure that STP is disabled on the port before assigning the port to a smart link group.

Examples

Configure link aggregation group 8 as the slave port of smart link group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] smart-link group 1
[Sysname-smlk-group1] link-aggregation group 8 slave
```

port

Syntax

port *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number*

View

Smart link group view

Parameters

interface-type: Port type.

interface-number: Port number.

master: Specifies the specified port as the master port of the smart link group.

slave: Specifies the specified port as the slave port of the smart link group.

Description

Use the **port** command to assign the specified port to the smart link group.

Use the **undo port** command to remove the specified port from the smart link group.

The port you specified in this command cannot be a link aggregation group member port.

Besides assigning single ports to a smart link group, you can assign a link aggregation group (static or manual, but not dynamic) to a smart link group with the **link-aggregation group** command in smart link group view.

Note

Because Smart Link and STP cannot be enabled on an Ethernet port at the same time, you must make sure that STP is disabled on the port before assigning the port to a smart link group.

Examples

Configure GigabitEthernet 1/0/6 as the slave port of smart link group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] smart-link group 1
[Sysname-smlk-group1] port GigabitEthernet 1/0/6 slave
```

port smart-link group

Syntax

port smart-link group *group-id* { **master** | **slave** }

undo port smart-link group *group-id*

View

Ethernet port view

Parameters

group-id: Smart link group ID, in the range of 1 to 24.

master: Specifies the port as the master port of the smart link group.

slave: Specifies the port as the slave port of the smart link group.

Description

Use the **port smart-link group** command to assign the current port to a smart link group.

Use the **undo port smart-link group** command to remove the current port from the specified smart link group.

The port where you configure the command cannot be a link aggregation group member port.

Besides assigning single ports to a smart link group, you can assign a link aggregation group (static or manual, but not dynamic) to a smart link group with the **link-aggregation group** command in smart link group view.

Note

Because Smart Link and STP cannot be enabled on an Ethernet port at the same time, you must make sure that STP is disabled on the port before assigning the port to a smart link group.

Examples

Configure GigabitEthernet 1/0/3 as the master port of smart link group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port smart-link group 1 master
```

reset smart-link packets counter

Syntax

reset smart-link packets counter

View

User view

Parameters

None

Description

Use the **reset smart-link packets counter** command to clear the flush message statistics of Smart Link.

Examples

Clear the flush message statistics of Smart Link.

```
<Sysname> reset smart-link packets counter
```

smart-link flush enable

Syntax

- In Ethernet port view:

smart-link flush enable control-vlan *vlan-id*

undo smart-link flush enable

- In system view:

smart-link flush enable control-vlan *vlan-id* **port** *interface-type interface-number* [**to** *interface-type interface-number*]

undo smart-link flush enable port *interface-type interface-number* [**to** *interface-type interface-number*]

View

Ethernet port view, system view

Parameters

vlan-id: Control VLAN ID, in the range of 1 to 4,094.

Description

Use the **smart-link flush enable control-vlan** command to enable the current/specified port to process flush messages received on the specified control VLAN.

Use the **undo smart-link flush enable** command to disable the port from processing flush messages.

- The command executed in Ethernet port view has effect on the current port only.
- The command executed in system view has effect on the specified port only.

By default, no control VLAN is specified.

If you configure different control VLANs on the same port, only the last one takes effect.

 **Note**

The VLAN configured as a control VLAN for sending or receiving flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as a control VLAN for the smart link group, this VLAN will become a static VLAN, and related prompt information is displayed.

Examples

Enable GigabitEthernet 1/0/4 to process flush messages received from control VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] smart-link flush enable control-vlan 1
```

Enable GigabitEthernet 1/0/5 through GigabitEthernet 1/0/10 to process flush messages received from control VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/5 to
GigabitEthernet 1/0/10
```

smart-link group

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

View

System view

Parameters

group-id: Smart link group ID, in the range of 1 to 24.

Description

Use the **smart-link group** command to create a smart link group and enter smart link group view. If the specified smart link group exists, this command leads you into smart link group view directly.

Use the **undo smart-link group** command to remove the specified smart link group.

After creating a smart link group, you must configure member ports for this smart link group.

Related commands: **port smart-link group**, **link-aggregation group**, **port**.

Note

Make sure that the smart link group has no members before executing the **undo smart-link group** command.

Examples

Create a smart link group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] smart-link group 1
 New Smart Link Group has been created.
[Sysname-smlk-group1]
```

2 Monitor Link Configuration Commands

Monitor Link Configuration Commands

display monitor-link group

Syntax

display monitor-link group { *group-id* | **all** }

View

Any view

Parameters

group-id: Monitor link group ID, ranging 1 to 24.

all: Specifies all the monitor link groups.

Description

Use the **display monitor-link group** command to display monitor link group information.

Examples

Display the information about monitor link group 1.

```
<Sysname> display monitor-link group 1
Monitor link group 1 information:
Member  Role       Status     Last-up-time          Last-down-time
--------------------------------------------------------------------
SMLK-2  UPLINK     UP         16:37:20 2006/4/21   16:37:20 2006/4/20
AGG-1   DOWNLINK   UP
```

Table 2-1 Description on the fields of the **display monitor-link group** command

Field	Description
Member	Member of the monitor link group
Role	Role of monitor link group member port: UPLINK or DOWNLINK
Status	Status of monitor link group member port: UP or DOWN
Last-up-time	Last time the port is up
Last-down-time	Last time the port is down

link-aggregation group

Syntax

link-aggregation group *group-id* { **uplink** | **downlink** }

undo link-aggregation group *group-id*

View

Monitor link group view

Parameters

group-id: Link aggregation group ID, ranging from 1 to 50 (A link aggregation group can be a manual or static link aggregation group only).

uplink: Specifies the specified link aggregation group as the uplink port of the monitor link group

downlink: Specifies the specified link aggregation group as the downlink port of the monitor link group

Description

Use the **link-aggregation group** command to configure the specified link aggregation group as a monitor link group member.

Use the **undo link-aggregation group** command to remove the specified link aggregation group from the current monitor link group.

In Monitor Link, a monitor link group member can be a single port, a manual or static link aggregation group, but not a dynamic link aggregation group. Uplink port can also be a smart link group.

Use this command only on the link aggregation groups that are not smart link group members.

Note

A port or a link aggregation group cannot serve as a member port for two smart link groups. On the other hand, a port or a link aggregation group cannot serve as a member of a smart link group and a monitor link group at the same time. However, a smart link group can serve as the uplink member port of a monitor link group.

Examples

Configure link aggregation group 8 as the downlink port of the monitor link group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] link-aggregation group 8 downlink
```

monitor-link group

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

View

System view

Parameters

group-id: Monitor link group ID, ranging from 1 to 24.

Description

Use the **monitor-link group** command to create a monitor link group and enter monitor link group view. If the monitor link group has been created, you enter the monitor link group view directly.

Use the **undo monitor-link group** command to remove a monitor link group.

After the monitor link group is configured, member ports of the monitor link group need to be configured.

Related commands: **port monitor-link group**, **link-aggregation group**, **smart-link group**, **port**.

Note

Make sure that the monitor link group has no members before executing the **undo monitor-link group** command.

Examples

Create a monitor link group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] monitor-link group 1
 New Monitor Link Group has been created.
[Sysname-mtlk-group1]
```

port

Syntax

port *interface-type interface-number* { **uplink** | **downlink** }

undo port *interface-type interface-number*

View

Monitor link group view

Parameters

interface-type: Port type.

interface-number: Port number.

uplink: Specifies the specified port as the uplink port of the monitor link group

downlink: Specifies the specified port as the downlink port of the monitor link group

Description

Use the **port** command to configure the specified port as a member of the monitor link group.

Use the **undo port** command to remove the specified port from the current monitor link group.

In Monitor Link, a monitor link group member can be a single port, a static link aggregation group, but not a dynamic link aggregation group. The uplink port of a monitor link group can also be a smart link group.

Do not use this command on member ports of a link aggregation group or a smart link group.

Note

A port or a link aggregation group cannot serve as a member port for two smart link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a smart link group and a monitor link group at the same time. However, a smart link group can serve as the uplink member port of a monitor link group.

Examples

Configure GigabitEthernet 1/0/7 as a downlink port of the monitor link group

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port GigabitEthernet 1/0/7 downlink
```

port monitor-link group

Syntax

port monitor-link group *group-id*{ **uplink** | **downlink** }

undo port monitor-link group *group-id*

View

Ethernet port view

Parameters

group-id: Monitor link group ID, ranging 1 to 24.

uplink: Specifies the port as the uplink port of the specified monitor link group

downlink: Specifies the port as the downlink port of the specified monitor link group

Description

Use the **port monitor-link group** command to configure the current port as a member of the specified monitor link group.

Use the **undo port monitor-link group** command to remove the current port from the specified monitor link group.

In Monitor Link, a monitor link group member can be a single port, a static link aggregation group, but not a dynamic link aggregation group. Uplink port can also be a smart link group.

Do not use this command on member ports of a link aggregation group or a smart link group.

Note

A port or a link aggregation group cannot serve as a member port for two smart link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a smart link group and a monitor link group at the same time. However, a smart link group can serve as the uplink member port of a monitor link group.

Examples

Configure GigabitEthernet 1/0/8 as a downlink port of monitor link group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/8
[Sysname-GigabitEthernet1/0/8] port monitor-link group 1 downlink
```

smart-link group

Syntax

smart-link group *group-id* **uplink**

undo smart-link group *group-id*

View

Monitor link group view

Parameters

group-id: Smart link group ID, ranging 1 to 24.

uplink: Specifies the specified smart link group as the uplink port of the monitor link group

Description

Use the **smart-link group** command to configure the specified smart link group as the uplink port of the monitor link group.

Use the **undo smart-link group** command to remove the configuration.

A smart link group can belong to only one monitor link group and can be configured only as an uplink port of the monitor link group.

Examples

Configure smart link group 1 as the uplink port of monitor link group 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] smart-link group 1 uplink
```

Table of Contents

1 IPv6 Configuration Commands

Basic IPv6 Configuration Commands

display dns ipv6 dynamic-host

Syntax

display dns ipv6 dynamic-host

View

Any view

Parameters

None

Description

Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name information in the cache, including the domain name, IPv6 address, and TTL of the DNS entries.

You can use the **reset dns ipv6 dynamic-host** command to clear all IPv6 dynamic domain name information from the cache.

Examples

Display IPv6 dynamic domain name information in the cache.

```
<Sysname> display dns ipv6 dynamic-host
No. Domain-name           IPv6 Address                              TTL
1   aaa                   2001::2                                    6
```

Table 1-1 Description on the fields of the **display dns ipv6 dynamic-host** command

Field	Description
No.	Sequence number
Domain-name	Domain name
IPv6 Address	IPv6 address of the corresponding domain name
TTL	Time-to-live of the domain name in the cache in seconds

Note

When you use the **display dns ipv6 dynamic-host** command to check the IPv6 dynamic domain names in the cache, the system will display the first 21 characters of the domain names if they contain more than 21 characters. This is because the domain name displayed in the Domain-name field can be up to 21 characters in length.

display ipv6 fib

Syntax

display ipv6 fib

View

Any view

Parameters

None

Description

Use the **display ipv6 fib** command to display all the IPv6 FIB entries.

The switch looks up a matching IPv6 FIB entry for forwarding an IPv6 packet.

Examples

Display all the IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 5
 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
Destination:    ::1                                  PrefixLength : 128
NextHop    :    ::1                                  Flag         : HU
TimeStamp  :    Date- 5/7/2006, Time- 14:35:32
Interface  :    InLoopBack0
Destination:    FE80::                               PrefixLength : 10
NextHop    :    ::                                   Flag         : BU
TimeStamp  :    Date- 5/7/2006, Time- 14:35:32
Interface  :    NULL0
Destination:    2008::                               PrefixLength : 64
NextHop    :    2008::5500                           Flag         : U
TimeStamp  :    Date- 5/7/2006, Time- 14:35:32
Interface  :    Vlan-interface1
Destination:    2008::5500                           PrefixLength : 128
NextHop    :    ::1                                  Flag         : HU
TimeStamp  :    Date- 5/7/2006, Time- 14:35:32
Interface  :    InLoopBack0
```

```
Destination:    2001::                                  PrefixLength : 64
NextHop    :    2008::3610                              Flag         : GSU
TimeStamp  :    Date- 5/7/2006, Time- 14:35:32
Interface  :    Vlan-interface1
```

Table 1-2 Description on the fields of the **display ipv6 fib** command

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address to which a packet is forwarded
PrefixLength	Prefix length of the destination address
NextHop	Next hop address when a packet is forwarded to the destination
Flag	Route flag: “U” — Usable route “G” — Gateway route “H” — Host route “B” — Blackhole route “D” — Dynamic route “S” — Static route
TimeStamp	Generation time of an FIB entry
Interface	Interface from which a packet is forwarded

display ipv6 host

Syntax

display ipv6 host

View

Any view

Parameters

None

Description

Use the **display ipv6 host** command to display the mapping between host name and IPv6 address.

Related commands: **ipv6 host**.

Examples

Display the mapping between host name and IPv6 address.

```
<Sysname> display ipv6 host
Host                 Age          Flags  IPv6Address (es)
SWB                  0            static  2002::1
```

Table 1-3 Description on the fields of the **display ipv6 host** command

Field	Description
Host	Host name
Age	Time for the entry to live, displayed as 0 in the case of static configuration.
Flags	Flag indicating whether the entry is configured statically or acquired dynamically
IPv6Address (es)	IPv6 address corresponding to a host name

display ipv6 interface

Syntax

display ipv6 interface [*interface-type interface-number* | **brief**]

View

Any view

Parameters

interface-type: Interface type.

interface-number: Interface number.

brief: Displays the brief IPv6 information of an interface.

Description

Use the **display ipv6 interface** command to display the IPv6 information of a specified interface.

If no interface is specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type for which IPv6 addresses can be configured is displayed; if *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed.

If the **brief** keyword is specified, the brief IPv6 information of the interface is displayed.

Examples

Display the IPv6 information of a VLAN interface.

```
<Sysname> display ipv6 interface Vlan-interface 1
Vlan-interface1 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE00:C
  Global unicast address(es):
    2008::5500, subnet is 2008::/64
  Joined group address(es):
    FF02::1:FF00:5500
    FF02::1:FF00:C
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 5
```

```
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

Table 1-4 Description on the fields of the **display ipv6 interface** command

Field	Description
Vlan-interface1 current state	VLAN interface link state: • Administratively DOWN: Indicates the VLAN interface is administratively down; that is, the interface is shut down using the **shutdown** command. • DOWN: Indicates the VLAN interface is administratively up but its physical state is down; that is, no ports in the VLAN are up, which may be caused by a link failure. • UP: Indicates the administrative and physical states of the VLAN interface are both up.
Line protocol current state	Link layer protocol state of an interface: • DOWN: Indicates the link layer protocol state of the VLAN interface is down, generally because no IP address is configured. • UP: Indicates the link layer protocol state of the VLAN interface is up.
IPv6 is enabled	IPv6 forwarding state of an interface (after an IPv6 address is configured for an interface, IPv6 is automatically enabled on it; IPv6 is enabled in the example)
link-local address	Link-local address configured on an interface
Global unicast address(es)	Aggregatable global unicast address configured on an interface
Joined group address(es)	Address of the multicast group that an interface joins
MTU	Maximum transmission unit of an interface
ND DAD is enabled, number of DAD attempts	Number of duplicate address detection (DAD) attempts, with DAD enabled • If DAD is enabled, the number of neighbor request messages is also displayed (configured by using the **ipv6 nd dad attempts** command) • If DAD is disabled, “ND DAD is disabled” is displayed. (You can set the number of neighbor request messages for DAD to 0 to disable this function.)
ND reachable time	Neighbor reachable time (which can be configured by using the **ipv6 nd nud reachable-time** command)
ND retransmit interval	Interval for retransmitting a neighbor solicitation (NS) message (which can be configured by using the **ipv6 nd ns retrans-timer** command)
Hosts use stateless autoconfig for addresses	Hosts use stateless auto-configuration mode to acquire IPv6 addresses

#: View the brief IPv6 information of all interfaces.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                              Physical   Protocol   IPv6 Address
Vlan-interface1                          up         up       2008::5500
```

Table 1-5 Description on the fields of the **display ipv6 interface brief** command

Field	Description
*down: administratively down	The interface is down, that is, the interface is disabled by using the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface
Physical	Interface link state: • *down: Indicates the VLAN interface is administratively down; that is, the interface is shut down using the **shutdown** command. • down: Indicates the VLAN interface is administratively up but its physical state is down; that is, no port in the VLAN is up, which may be caused by a link failure. • up: Indicates the administrative and physical states of the VLAN interface are both up.
Protocol	Link protocol state of an interface • down: Indicates the link layer protocol state of the VLAN interface is down, generally because no IP address is configured. • up: Indicates the link layer protocol state of the VLAN interface is up.
IPv6 Address	IPv6 address of the interface (If no address is configured for the interface, “Unassigned” will be displayed.)

display ipv6 neighbors

Syntax

display ipv6 neighbors { *ipv6-address* | **all** | **dynamic** | **static** | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Parameters

ipv6-address: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

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, in the range of 1 to 4094.

|: Uses a regular expression to match neighbor entries.

regular-expression: A case-sensitive string for matching.

- **begin**: Displays the first matching neighbor entry and all the neighbor entries following it.
- **exclude**: Displays the neighbor entries not matching the specified regular expression.

- **include**: Displays the neighbor entries matching the specified regular expression.

The regular expression supports various special characters. For details, refer to the **display current-configuration** command in *Configuration File Management Command*.

Description

Use the **display ipv6 neighbors** command to display neighbor information.

You can use the **reset ipv6 neighbors** command to clear specific IPv6 neighbor information.

Related commands: **ipv6 neighbor**, **reset ipv6 neighbors**.

Examples

View all neighbor information.

```
<Sysname> display ipv6 neighbors all
                Type: S-Static    D-Dynamic
IPv6 Address                Link-layer     VID  Interface    State T Age
2008::110                   0015-e9ac-69b6 1    GE1/0/2      REACH S -
FE80::215:E9FF:FEAC:69B6    0015-e9ac-69b6 1    GE1/0/3      STALE D 22
FE80::20F:E2FF:FE00:2201    000f-e200-2201 1    GE1/0/4      STALE D 28
2008::3610                  000f-e200-2201 1    GE1/0/5      STALE D 28
```

Table 1-6 Description on the fields of the **display ipv6 neighbors** command

Field	Description
IPv6 Address	IPv6 address of a neighbor
Link-layer	Link layer address (MAC address of a neighbor)
VID	ID of the VLAN to which the interface connected to a neighbor belongs
Interface	Interface connected to a neighbor
State	State of a neighbor, which can be: • INCMP: Address resolution is in progress, so the link layer address of the neighbor is unknown yet. • REACH: The neighbor is reachable. • STALE: The reachability to the neighbor is unknown. The device does not verify the reachability to the neighbor unless it sends a packet to the neighbor. • DELAY: The reachability to the neighbor is unknown. The device will send a neighbor request message after a delay time. • PROBE: The reachability to the neighbor is unknown. The device sent a neighbor request message to verify the reachability.
T	Type of neighbor information, including S (static configuration) and D (dynamic acquisition).
Age	• For a static entry, “-“ is displayed. • For a dynamic entry, the time (in seconds) since it is reachable last time is displayed, and if it is never reachable, “#” is displayed (for a dynamic neighbor only).

display ipv6 neighbors count

Syntax

display ipv6 neighbors { **all** | **dynamic** | **static** | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

View

Any view

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 all neighbor entries configured statically.

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, in the range of 1 to 4,094.

count: Number of neighbor entries.

Description

Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

Examples

Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  3
```

display ipv6 route-table

Syntax

display ipv6 route-table [**verbose**]

View

Any view

Parameters

verbose: Displays detailed information about the IPv6 routing table.

Description

Use the **display ipv6 route-table** command to display brief information about the routing table, including the destination IP address, prefix length, type of protocol, next hop, egress interface, and so on. In this case, only the valid route entries are displayed,

Use the **display ipv6 route-table verbose** command to display detailed information about the routing table. In this case, both valid routes and invalid routes are displayed.

Examples

Display summary information about the routing table.

```
<Sysname> display ipv6 route-table

Routing Table:
Destinations : 4      Routes : 4

Destination: ::1/128                                    Protocol: Direct
NextHop    : ::1
Interface  : InLoopBack0

Destination: 2008::/64                                  Protocol: Direct
NextHop    : 2008::32
Interface  : Vlan-interface1

Destination: 2008::32/128                               Protocol: Direct
NextHop    : ::1
Interface  : InLoopBack0

Destination: FE80::/10                                  Protocol: Direct
NextHop    : ::
Interface  : NULL0
```

Table 1-7 Description on the fields of the **display ipv6 route-table** command

Field	Description
Destinations	Number of reachable destination networks/hosts
Routes	Number of routing entries
Destination	Destination network/host IPv6 address. The part following “/” indicates the prefix length.
Protocol	Routing protocol discovering the route
NextHop	Next hop address
Interface	Egress interface, through which a packet is sent.

Display detailed information about the routing table.

```
<Sysname> display ipv6 route-table verbose

Routing Table:
Destinations : 2      Routes : 2

Destination: ::                                 PrefixLength: 0
NextHop    : 1:1:4::1                           Protocol    : Static
Interface  : Vlan-interface1                       State        : Active

Destination: ::1                                PrefixLength: 128
NextHop    : ::1                                Protocol    : Direct
```

```
Interface  : InLoopBack0                          State      : Active
```

Table 1-8 Description on the fields of the **display ipv6 route-table verbose** command

Field	Description
Destinations	Number of reachable destination networks/hosts
Routes	Number of routing entries
Destination	Destination network/host IPv6 address.
PrefixLength	Prefix length of the destination IPv6 address
NextHop	Next hop address
Protocol	Routing protocol discovering the route
Interface	Egress interface
State	Routing entry state: Active (valid route) or Inactive (invalid route).

display ipv6 socket

Syntax

display ipv6 socket [**socktype** *socket-type*] [*task-id socket-id*]

View

Any view

Parameters

socket-type: Type of a socket, in the range of 1 to 3. The value “1” represents a TCP socket, “2” a UDP socket, and “3” a raw IP socket.

task-id: ID of a task, in the range of 1 to 100.

socket-id: ID of a socket, in the range of 0 to 3072.

Description

Use the **display ipv6 socket** command to display information related to a specified socket.

With no argument 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 information related to a specified socket.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYD(43), socketid = 1, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_KEEPALIVE SO_REUSEPORT SO_SETKEEPALIVE,
```

```
socket state = SS_PRIV SS_ASYNC
SOCK_DGRAM:
SOCK_RAW:
```

Table 1-9 Description on the fields of the **display ipv6 socket** command

Field	Description
SOCK_STREAM	Socket type, which can be: • SOCK_STREAM: Refers to TCP. • SOCK_DGRAM: Refers to UDP. • SOCK_RAW: Refers to raw IP.
Task	Task name and ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the sending buffer
rcvbuf	Size of the receiving buffer
sb_cc	Number of bytes sent by the sending buffer
rb_cc	Number of bytes received by the receiving buffer
socket option	Socket option set by the application
socket state	State of the socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket

display ipv6 statistics

Syntax

display ipv6 statistics

View

Any view

Parameters

None

Description

Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets.

You can use the **reset ipv6 statistics** command to clear all IPv6 and ICMPv6 packet statistics.

Examples

View the statistics of IPv6 packets and IPv6 ICMP packets.

```
<Sysname> display ipv6 statistics
```

```
IPv6 Protocol:
  Sent packets:
    Total:      580
      Local sent out:       550          forwarded:           0
      raw packets:          30           discarded:           0
      routing failed:       0            fragments:           0
      fragments failed:     0
  Received packets:
    Total:      572
      local host:           572          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:      132
      unreached:           0             too big:              0
      hopcount exceeded:   0             reassembly timeout:   0
      parameter problem:   0
      echo request:        30            echo replied:         17
      neighbor solicit:    43            neighbor advert:      42
      router solicit:      0             router advert:        0
      redirected:          0
    Send failed:
      ratelimited:         0             other errors:         0
  Received packets:
    Total:      126
      checksum error:      0             too short:            0
      bad code:            0
      unreached:           10            too big:              0
      hopcount exceeded:   0             reassembly timeout:   0
      parameter problem:   0             unknown error type:   0
      echoed:              17            echo replied:         30
      neighbor solicit:    34            neighbor advert:      35
      router solicit:      0             router advert:        0
      redirected:          0             router renumbering:   0
      unknown info type:   0
    Deliver failed:
      bad length:          0             ratelimited:          0
```

Table 1-10 Description on the fields of the **display ipv6 statistics** command

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets

Field	Description
Sent packets: Total: 580 Local sent out: 550 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: • Total number of sent packets • Number of packets sent locally • Number of forwarded packets • Number of packets sent via raw socket • Number of discarded packets • Number of packets with routing failure • Number of sent fragment packets • Number of fragment sending failures
Received packets: Total: 572 local host: 572 hopcount exceeded: 0 format error: 0 option error: 0 protocol error: 0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets, including: • Total number of received packets • Number of packets received locally • Number of packets exceeding the hops • 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 whose reassembly fails • Number of packets whose reassembly times out
ICMPv6 protocol:	Statistics of ICMPv6 packets
Sent packets: Total: 132 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 30 echo replied: 17 neighbor solicit: 43 neighbor advert: 42 router solicit: 0 router advert: 0 redirected: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of sent ICMPv6 packets, including: • Total number of sent packets • Number of packets whose destination is unreachable • Number of too large packets • Number of packets exceeding the hop limit • Number of packets whose fragmentation and reassembly time out • Number of packets with parameter errors • Number of request packets • Number of response packets • Number of neighbor solicitation packets • Number of neighbor advertisement packets • Number of router solicit packets • Number of router advertisement packets • Number of redirected packets • Number of packets failing to be sent because of rate limitation • Number of packets with other errors

Field	Description
Received packets: Total: 126 checksum error: 0 too short: 0 bad code: 0 unreached: 10 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echoed: 17 echo replied: 30 neighbor solicit: 34 neighbor advert: 35 router solicit: 0 router advert: 0 redirected: 0 router renumbering: 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets, including: • Total number of received packets • Number of packets with checksum errors • Number of too small packets • Number of packets with error codes • Number of packets whose destination is unreachable • Number of too large packets • Number of packets exceeding the hop limit • Number of packets whose fragmentation and reassembly time out • Number of packets with parameter errors • Number of packets with unknown errors • Number of request packets • Number of response packets • Number of neighbor solicitation messages • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of redirected packets • Number of packets recounted by the router • Number of unknown information type of packets • Number of packets with a incorrect size • Number of packets failing to be received because of rate limitation

display tcp ipv6 statistics

Syntax

display tcp ipv6 statistics

View

Any view

Parameters

None

Description

Use the **display tcp ipv6 statistics** command to display statistics of IPv6 TCP packets.

You can use the **reset tcp ipv6 statistics** command to clear statistics of all IPv6 TCP packets.

Examples

View the statistics of received and sent IPv6 TCP packets.

```
<Sysname> display tcp ipv6 statistics
Received packets:
     Total: 436
     packets in sequence: 182 (327 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: 3 (0 bytes)
     packets with data after window: 0 (0 bytes)
     packets after close: 0
     ACK packets: 239 (6141 bytes)
     duplicate ACK packets: 69, too much ACK packets: 0
Sent packets:
     Total: 331
     urgent packets: 0
     control packets: 5 (including 0 RST)
     window probe packets: 0, window update packets: 0
     data packets: 306 (6135 bytes) data packets retransmitted: 0 (0 bytes)
     ACK only packets: 20 (14 delayed)
Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 66, keepalive probe: 66, Keepalive timeout, so connections disconnected :
0
Initiated connections: 2, accepted connections: 3, established connections: 3
Closed connections: 5 (dropped: 0, initiated dropped: 2)
```

Table 1-11 Description on the fields of the **display tcp ipv6 statistics** command

Field	Description
Received packets: Total: 436 packets in sequence: 182 (327 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: 3 (0 bytes) packets with data after window: 0 (0 bytes) packets after close: 0 ACK packets: 239 (6141 bytes) duplicate ACK packets: 69, too much ACK packets: 0	Statistics of received packets, including: • Total number of received packets • Number of packets received in sequence • Number of window probe packets • Number of window size update packets • Number of packets with checksum errors • Number of packets with offset errors • Number of packets whose total length is less than that 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 receiving window size • Number of packets after the connection is closed • Number of ACK packets • Number of duplicate ACK packets • Number of excessive ACK packets

Field	Description
Sent packets: Total: 331 urgent packets: 0 control packets: 5 (including 0 RST) window probe packets: 0, window update packets: 0 data packets: 306 (6135 bytes) data packets retransmitted: 0 (0 bytes) ACK only packets: 20 (14 delayed)	Statistics of sent packets, including: • Total number of packets • Number of packets containing an urgent indicator • Number of control packets • Number of window probe packets • Number of window update packets • Number of data packets • Number of retransmitted packets • Number of ACK only packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
Keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after receiving SYN from the peer)
initiated dropped	Number of connection failures (before receiving SYN from the peer)

display tcp ipv6 status

Syntax

display tcp ipv6 status

View

Any view

Parameters

None

Description

Use the **display tcp ipv6 status** command to display the IPv6 TCP connection status, including IP address of the IPv6 TCP control block, local and peer IPv6 addresses, and status of the IPv6 TCP connection.

Examples

View the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB   Local Address            Foreign Address          State
83a9fba4 ::->23                   ::->0                    Listening
```

Table 1-12 Description on the fields of the **display tcp ipv6 status** command

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address
State	TCP connection status, including: Closed, Listening, Syn_Sent, Syn_Rcvd, Established, Close_Wait, Fin_Wait1, Closing, Last_Ack, Fin_Wait2, Time_Wait

display udp ipv6 statistics

Syntax

display udp ipv6 statistics

View

Any view

Parameters

None

Description

Use the **display udp ipv6 statistics** command to display statistics of IPv6 UDP packets.

You can use the **reset udp ipv6 statistics** command to clear statistics of all IPv6 UDP packets.

Examples

View statistics of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
     Total: 10
     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: 21
```

Table 1-13 Description on the fields of the **display udp ipv6 statistics** command

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with an invalid checksum
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 on a port
broadcast/multicast(no socket on port)	Total number of received broadcast/multicast packets without any socket on a port
not delivered, input socket full	Number of packets not handled because of the receiving buffer being full
input packet missing pcb cache	Number of packets that do not match any entry in the PCB cache

dns server ipv6

Syntax

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View

VLAN interface view

Parameters

ipv6-address: IPv6 address of a DNS server.

interface-type interface-number: Interface type and interface number. It is required when the IPv6 address of the specified DNS server is a link-local address.

Description

Use the **dns server ipv6** command to configure an IPv6 address for a DNS server.

Use the **undo dns server ipv6** command to remove the configured DNS server.

By default, no DNS server is configured.

Examples

Configure the IPv6 address 2002::1 for a DNS server.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dns server ipv6 2002::1
```

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

Parameters

ipv6-address: IPv6 address.

prefix-length: Prefix length of an IPv6 address, in the range of 1 to 128.

Description

Use the **ipv6 address** command to configure a site-local address or global unicast address manually for an interface.

Use the **undo ipv6 address** command to remove the manually configured interface address.

By default, no site-local address or global unicast address is configured for an interface.

Note that:

- A 3com switch 4200G can have IPv6 unicast addresses configured on only one VLAN interface. The total number of IPv6 global unicast addresses and site-local addresses configured on an interface can be up to four.
- You will remove all IPv6 addresses except the automatically configured link-local address if you carry out the **undo ipv6 address** command without any parameter specified.

Examples

Set the aggregatable global IPv6 unicast address of VLAN-interface 1 to 2001::1 with prefix length 64.

Method I:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64
```

Method II:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1 64
```

ipv6 address auto link-local

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

View

VLAN interface view

Parameters

None

Description

Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for an interface.

By default, a link-local address is generated automatically after a site-local IPv6 address or global unicast address is configured for an interface.

Note that:

- After an IPv6 site-local address or aggregatable global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The **undo ipv6 address auto link-local** command can be used only after the **ipv6 address auto link-local** command is executed. However, if an IPv6 site-local address or aggregatable global unicast address is already configured for an interface, the interface still has a link-local address because the system automatically generates one for the interface. If no IPv6 site-local address or aggregatable global unicast address is configured, the interface has no link-local address.
- Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For manually assignment of an IPv6 link-local address, refer to the **ipv6 address link-local** command.

Examples

Configure the VLAN-interface 1 to automatically generate a link-local address.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] 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

VLAN interface view

Parameters

ipv6-address|*prefix-length*: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an IPv6 address in the EUI-64 format. The prefix length of an EUI-64 address cannot be greater than 64.

Description

Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for an interface.

By default, no site-local address or global unicast address in the EUI-64 format is configured on the interface.

An IPv6 address in the EUI-64 format consists of a specific prefix and the MAC address of the local device, which can be displayed using the **display ipv6 interface** command.

Note that:

The prefix length should not be more than 64 bits when a aggregatable global unicast address(es) or site-local address(es) in the EUI-64 format is configured.

Examples

Configure an IPv6 address in the EUI-64 format for the VLAN-interface 1. The prefix of the address is 2001::1/64, and the interface ID is generated based on the MAC address of the device.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64 eui-64
```

Display the generated IPv6 address in the EUI-64 format.

```
[Sysname-Vlan-interface1] display ipv6 interface Vlan-interface 1
Vlan-interface1 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE00:3100
  Global unicast address(es):
    2001::2E0:FCFF:FE00:3100, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:3100
    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
```

Configure VLAN-interface 1 to generate an IPv6 address in the EUI-64 format based on the prefix 3001::/64.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
```

```
[Sysname-Vlan-interface1] ipv6 address 3001::/64 eui-64
```

ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View

VLAN interface view

Parameters

ipv6-address: IPv6 link-local address. The first ten bits of an address must be 1111111010 (binary), that is, the first group of hexadecimals in the address must be FE80 to FEBF.

Description

Use the **ipv6 address link-local** command to configure a link-local address manually for a specified interface.

Use the **undo ipv6 address link-local** command to remove the configured link-local address for an interface.

Note that:

Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For automatic generation of an IPv6 link-local address, refer to the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for the VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address fe80::1 link-local
```

ipv6 host

Syntax

ipv6 host *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View

System view

Parameters

hostname: Host name, a string of up to 20 characters. The character string can contain letters, numerals, “_”, “-“, or “.” and must contain at least one letter.

ipv6-address: IPv6 address.

Description

Use the **ipv6 host** command to configure the mapping between host name and IPv6 address.

Use the **undo ipv6 host** command to remove the mapping between host name and IPv6 address.

Each host name can correspond to only one IPv6 address. A newly configured IPv6 address will overwrite the previous one.

Related commands: **display ipv6 host**.

Examples

Configure the mapping between host name and IPv6 address.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6 host aaa 2001::1
```

ipv6 icmp-error

Syntax

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* }*

undo ipv6 icmp-error

View

System view

Parameters

bucket-size: Number of tokens in a token bucket, in the range of 1 to 200. The default value is 10.

interval: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647.

Description

Use the **ipv6 icmp-error** command to configure the maximum number of IPv6 ICMP error packets sent within a specified time.

Use the **undo ipv6 icmp-error** command to restore the update period and the capacity of the token bucket to the defaults.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 IPv6 ICMP 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. That is, at most 50 IPv6 ICMP error packets can be sent within 100 milliseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

View

VLAN interface view

Parameters

value: Number of attempts to send a neighbor solicitation message for duplicate address detection, in the range of 0 to 600. The default value is “1”. When it is set to 0, the duplicate address detection is disabled.

Description

Use the **ipv6 nd dad attempts** command to configure the attempts to send a neighbor solicitation message for duplicate address detection.

Use the **undo ipv6 nd dad attempts** command to restore the attempts to send a neighbor solicitation message for duplicate address detection to the default.

By default, the number of attempts to send a neighbor solicitation message for duplicate address detection is 1.

Related commands: **display ipv6 interface**.

Examples

Set the attempts to send a neighbor solicitation message for duplicate address detection to 20.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax

ipv6 nd hop-limit *value*

undo ipv6 nd hop-limit

View

System view

Parameters

value: Number of hops, in the range of 0 to 255.

Description

Use the **ipv6 nd hop-limit** command to configure the hop limit of ICMPv6 reply packets.

Use the **undo ipv6 nd hop-limit** command to restore the default.

By default, the hop limit of ICMPv6 reply packets is 64.

Examples

Set the hop limit of ICMPv6 reply packets to 100.

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

VLAN interface view

Parameters

value: Interval for retransmitting an NS message in milliseconds, in the range of 1,000 to 3,600,000.

Description

Use the **ipv6 nd ns retrans-timer** command to set the interval for retransmitting an NS message.

Use the **undo ipv6 nd ns retrans-timer** command to restore the interval for retransmitting an NS message to the default.

By default, the local interface sends NS messages at intervals of 1,000 milliseconds

Related commands: **display ipv6 interface**.

Examples

Specify the VLAN-interface 1 to send an NS message at intervals of 10,000 milliseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] 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

VLAN interface view

Parameters

value: Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.

Description

Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds.

Related commands: **display ipv6 interface**.

Examples

Set the neighbor reachable time on the VLAN-interface 1 to 10,000 milliseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd nud reachable-time 10000
```

ipv6 neighbor

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

View

System view

Parameters

ipv6-address: IPv6 address in a static neighbor entry.

mac-address: Link layer address in a static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: VLAN ID corresponding to a static neighbor entry, in the range of 1 to 4094.

port-type port-number: Ethernet port type and port number corresponding to a static neighbor entry.

interface-type interface-number: VLAN interface type and interface number corresponding to a static neighbor entry.

Description

Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

Note that:

You can configure a static neighbor entry in two ways:

- Mapping a VLAN interface to an IPv6 address and a link-layer address. The entry state is INCMP. After the switch get the layer 2 port information of the VLAN, the neighbor entry enters the REACH state.
- Mapping a Layer 2 port in a VLAN to an IPv6 address and a link-layer address. The Layer 2 port specified by the *port-type port-number* argument must belong to the VLAN specified by the *vlan-id* argument, and the corresponding VLAN interface must exist. After you carry out the command, the

device relates the VLAN interface to the IPv6 address to uniquely identify a static neighbor entry which is in REACH state.

You only need to specify the corresponding VLAN interface when removing a static neighbor entry related to that VLAN interface.

Related commands: **display ipv6 neighbors**.

Examples

Configure a static neighbor entry for GigabitEthernet 1/0/1 of VLAN 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 1 GigabitEthernet 1/0/1
```

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

VLAN interface view

Parameters

number: Maximum number of neighbors that can be dynamically learned by an interface, in the range of 1 to 2048.

Description

Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on a specified interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the configuration to the default.

By default, the maximum number is 1024.

Examples

Set the maximum number of neighbors that can be dynamically learned on the interface VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ipv6 neighbors max-learning-num 10
```

ipv6 route-static

Syntax

ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] *nexthop-address*

undo ipv6 route-static *ipv6-address prefix-length*

View

System view

Parameters

ipv6-address prefix-length: Destination IPv6 address and prefix length.

interface-type interface-number: Type of egress interface and interface number.

nexthop-address: IPv6 address of the next hop.

Description

Use the **Ipv6 route-static** command to configure a static IPv6 route.

Use the **undo ipv6 route-static** command to remove a static IPv6 route.

By default, no IPv6 static route is configured.

If you specify the destination IP address of an IPv6 static route as ::/0, the route configured becomes a default IPv6 route. If the destination IP address of a packet does not match any entry in the routing table, the device will use a default IPv6 route to forward the IPv6 packet.

Related commands: **display ipv6 route-table**.

Examples

Configure a static IPv6 route, with the destination address of 1:1:2::/48 and the next hop address of 1:1:3::1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6 route-static 1:1:2:: 48 1:1:3::1
```

Configure a static IPv6 route, with the next hop address of 1:1:4::1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] ipv6 route-static :: 0 1:1:4::1
```

reset dns ipv6 dynamic-host

Syntax

reset dns ipv6 dynamic-host

View

User view

Parameters

None

Description

Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

You can use the **display dns ipv6 dynamic-host** command to display the current IPv6 dynamic domain name cache information.

Examples

Clear IPv6 dynamic domain name cache information.

```
<Sysname> reset dns ipv6 dynamic-host
```

reset ipv6 neighbors

Syntax

reset ipv6 neighbors [**all** | **dynamic** | **interface** *interface-type interface-number* | **static**]

View

User view

Parameters

all: Clears the static and dynamic neighbor information on all interfaces.

dynamic: Clears the dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears all neighbor information of a specified interface.

static: Clears the static neighbor information on all interfaces.

Description

Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

You can use the **display ipv6 neighbors** command to display the current IPv6 neighbor information.

Examples

Clear all neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

Clear dynamic neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

Clear all neighbor information on VLAN-interface 1.

```
<Sysname> reset ipv6 neighbors interface Vlan-interface 1
```

reset ipv6 statistics

Syntax

reset ipv6 statistics

View

User view

Parameters

None

Description

Use the **reset ipv6 statistics** command to clear the statistics of IPv6 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.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax

reset tcp ipv6 statistics

View

User view

Parameters

None

Description

Use the **reset tcp ipv6 statistics** command to clear the statistics of all IPv6 TCP packets.

You can use the **display tcp ipv6 statistics** command to display the statistics of IPv6 TCP packets.

Examples

Clear the statistics of all IPv6 TCP packets.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax

reset udp ipv6 statistics

View

User view

Parameters

None

Description

Use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

You can use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

Examples

Clear the statistics of all IPv6 UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax

tcp ipv6 timer fin-timeout *wait-time*

undo tcp ipv6 timer fin-timeout

View

System view

Parameters

wait-time: Length of the finwait timer of IPv6 TCP packets in seconds, in the range of 76 to 3,600.

Description

Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer of IPv6 TCP packets

Use the **undo tcp ipv6 timer fin-timeout** command to restore the finwait timer length to the default.

By default, the length of the finwait timer is 675 seconds.

Examples

Set the finwait timer length of IPv6 TCP packets 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

Parameters

wait-time: Length of the synwait timer of IPv6 TCP packets in seconds, in the range of 2 to 600.

Description

Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer of IPv6 TCP packets

Use the **undo tcp ipv6 timer syn-timeout** command to restore the synwait timer length to the default.

By default, the length of the synwait timer of IPv6 TCP packets is 75 seconds.

Examples

Set the synwait timer length of IPv6 TCP packets to 800 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tcp ipv6 timer syn-timeout 800
```

tcp ipv6 window

Syntax

tcp ipv6 window *size*

undo tcp ipv6 window

View

System view

Parameters

size: size of IPv6 TCP receiving/sending buffer in KB (kilobyte), in the range of 1 to 32.

Description

Use the **tcp ipv6 window** command to set the size of IPv6 TCP receiving/sending buffer.

Use the **undo tcp ipv6 window** command to restore the size of IPv6 TCP receiving/sending buffer to the default.

By default, the size of the IPv6 TCP packet buffer is 8 KB.

Examples

Set the size of IPv6 TCP receiving/sending buffer to 4 KB.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] tcp ipv6 window 4
```

2 IPv6 Application Configuration Commands

IPv6 Application Configuration Commands

ping ipv6

Syntax

ping ipv6 [**-a** *source-ipv6-address* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout*]* *remote-system* [**-i** *interface-type interface-number*]

View

Any view

Parameters

-a *source-ipv6-address*: Specifies source IPv6 address.

-c *count*: Specifies the number of packets sent for requesting ICMPv6 echo, ranging from 1 to 4294967295, with the default of 5.

-m *interval*: Specifies the time intervals in milliseconds to send packets for ICMPv6 echo, ranging from 1 to 65,535, with the default of 200 milliseconds.

- If a response from the destination is received within the timeout time, the interval to send the next ECHO-REQUEST equals to 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 to the *timeout* value plus the value of *interval.*

-s *packet-size*: Specifies the size in bytes of packets sent for requesting ICMPv6 echo, ranging from 20 to 8,100, with the default of 56 bytes.

-t *timeout*: Specifies the timeout in milliseconds of receiving ICMPv6 echoes, ranging from 0 to 65,535, with the default of 2,000 milliseconds.

remote-system: IPv6 address or host name (a string a 1 to 46 characters) of the destination device.

-i *interface-type interface-number*: Specifies the type and number of an outgoing interface. This argument takes effect only when the destination address is a link-local address and the specified outgoing interface has a link-local address.

Description

Use the **ping ipv6** command to test whether the destination is accessible.

The following information will be output:

- A reply to each ICMPv6 echo request. If no ICMPv6 reply is received within the timeout time, “Request time out” is displayed; otherwise, the number of data bytes of each reply, packet sequence number, TTL, and round-trip response time are displayed.
- Statistics, including the numbers of sent packets, received packets, packet loss percentage, and the minimum/average/maximum response time.

After you execute the **ping ipv6** command, you can press **Ctrl+C** to terminate the ping operation.

Examples

Test whether destination 2001::1 is accessible.

```
<Sysname> ping ipv6 2001::1
  PING 2001::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64  time = 20 ms
    Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64  time = 0 ms
    Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64  time = 0 ms
    Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64  time = 0 ms
    Reply from 2001::1
    bytes=56 Sequence=5 hop limit=64  time = 0 ms

  --- 2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 0/4/20 ms
```

Table 2-1 Description on the fields of the **ping ipv6** command

Field	Description
PING 2001::1	Verify whether the device at 2001::1 is reachable
56 data bytes	Number of bytes in the ICMPv6 echo request
press CTRL_C to break	Press **Ctrl + C** to terminate the ping operation after the **ping ipv6** command is executed.
Reply from 2001::1	An ICMPv6 reply message is received from the device at 2001::1. If no ICMPv6 reply is received within the timeout time, “Request time out” is displayed.
bytes=	Number of data bytes in the ICMPv6 reply message
Sequence=	Packet sequence number
hop limit=	TTL in the ICMP reply message, similar to the TTL in the output information of IPv4 ping operations.
time =	Round-trip response time
--- 2001::1 ping statistics ---	Statistics obtained by pinging the IPv6 address 2001::1
5 packet(s) transmitted	Number of sent packets
5 packet(s) received	Number of received packets
0.00% packet loss	Packet loss percentage
round-trip min/avg/max = 0/4/20 ms	Minimum/average/maximum response time, in milliseconds.

telnet ipv6

Syntax

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

View

User view

Parameters

remote-system: IPv6 address or host name (a string a 1 to 46 characters) of the destination device.

-i *interface-type interface-number*: Specifies the type and number of an outgoing interface. This argument takes effect only when the destination address is a link-local address and the specified outgoing interface has a link-local address.

port-number: Specifies the port number linked with a Telnet server, ranging from 0 to 65535, with the default of 23.

Description

Use the **telnet ipv6** command to log onto another device for remote management from the local device. You can break Telnet logging-in by entering <Ctrl+K>.

Examples

Connect to a remote Telnet server with IPv6 address of 3001::1.

```
<Sysname> telnet ipv6 3001::1
Trying 3001::1 ...
Press CTRL+K to abort
Connected to 3001::1 ...
******************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.*
*  Without the owner's prior written consent,                                *
*  no decompiling or reverse-engineering shall be allowed.                   *
******************************************************************************


<Sysname>
```

Telnet to a remote Telnet server with IPv6 address of 2003::5. If the connection fails, “Can't connect to the remote host!” is displayed.

```
<Sysname> telnet ipv6 2003::5
Trying 2003::5 ...
Press CTRL+K to abort
Can't connect to the remote host!
```

tftp ipv6

Syntax

tftp ipv6 *remote-system* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]

View

User view

Parameters

remote-system: IPv6 address or host name (a string a 1 to 46 characters) of the destination device.

-i *interface-type interface-number*: Specifies the type and number of an interface. This argument takes effect only when the address of the TFTP server is a link-local address and the specified outgoing interface has a link-local address.

get: Specifies to download a file.

put: Specifies to upload a file.

source-filename: Specifies the name of a source file with a string of 1 to 64 letters.

destination-filename: Specifies the name of a destination file with a string of 1 to 64 letters. If no such parameters are specified, then the destination file's name will be the same as the source file's.

Description

Use the **tftp ipv6** command to perform the following operations:

- Download a file: Download a specified source file from TFTP server to local.
- Upload a file: Upload a specified source file from local to TFTP server.

Examples

Download a file from TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i Vlan-interface 300 get filetoget
  .
  File will be transferred in binary mode
  Downloading file from remote tftp server, please wait.....  received: 4469 bytes in 1.243
seconds.
```

tracert ipv6

Syntax

tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-num* | **-w** *timeout*]* *remote-system*

View

Any view

Parameters

-f *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet. Ranges from 1 to 255, defaults to 1, and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet. The value ranges from 1 to 255, defaults to 30. It must be greater than the first TTL.

-p *port*: Specifies the port number of the destination UDP, ranging from 1 to 65535, with the default of 33434.

-q *packet-num*: Specifies the maximum number of packets sent to a hop, ranging from 1 to 65535, with the default of 3.

-w *timeout*: Specifies the timeout in milliseconds of waiting ICMPv6 echoes, ranging from 1 to 65,535, with the default of 5,000 milliseconds.

remote-system: IPv6 address or host name (a string a 1 to 46 characters) of the destination device.

Description

Use the **tracert ipv6** command to trace the route of the IPv6 packets from source to destination.

After using the **ping** command to detect a network problem, you can use the **tracert** command to locate the failed network node.

Executing the **tracert** command displays the IP addresses of all the Layer 3 forwarding devices which forward the packets to the destination on the path; if a device times out, "* * *" is displayed.

You can press **Ctrl + C** to terminate the tracert operation after the **tracert ipv6** command is executed.

Examples

Trace the route of the IPv6 packets from source to destination 3002::1.

```
<Sysname> tracert ipv6 3002::1
 traceroute to 3002::1  30 hops max,60 bytes packet
 1 3003::1 30 ms  0 ms  0 ms
 2 3002::1 10 ms 10 ms 0 ms
 3  *  *  *
```

Table 2-2 Description on the fields of the **tracert ipv6** command

Field	Description
traceroute to 3002::1	Traceroute the device at 3002::1 to view the passed route
30 hops max	Maximum hops, which can be configured using the **-m** argument.
60 bytes packet	Number of bytes in a probe packet
press CTRL_C to break	Press **Ctrl + C** to terminate the tracert operation after the **tracert ipv6** command is executed.
1 3003::1 30 ms 0 ms 0 ms	Probe result for sending packets with TTL 1, including IPv6 address of the device and round-trip response times of three probe packets. The number of probe packets sent each time can be configured using the **-q** argument.
3 * * *	The device three hops away has no response.

Table of Contents

1 PoE Configuration Commands

PoE Configuration Commands

display poe disconnect

Syntax

display poe disconnect

View

Any view

Parameters

None

Description

Use the **display poe disconnect** command to view the current PD disconnection detection mode of the switch.

Examples

Display the PD disconnection detection mode.

```
<Sysname> display poe disconnect
The PoE disconnect mode is AC.
```

display poe interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display poe interface** command to view the PoE status of a specific port or all ports of the switch.

If the *interface-type interface-number* argument is not specified, the command displays the PoE status of all ports of the switch.

Related commands: **poe enable**, **poe max-power**, **poe mode**, **poe power-management**, **poe priority**.

Examples

Display the PoE status of GigabitEthernet 1/0/10.

```
<Sysname> display poe interface GigabitEthernet1/0/10
Port power enabled           :enable
Port power ON/OFF            :on
Port power status            :Standard PD was detected
Port power mode              :signal
Port PD class                :0
port power priority          :low
Port max power               :15400 mW
Port current power           :460 mW
Port peak power              :552 mW
Port average power           :547 mW
Port current                 :10 mA
Port voltage                 :51 V
```

Table 1-1 display poe interface command output description

Field	Description
Port power enabled	PoE is enabled on the port
Port power ON/OFF	The power on the port is on/off
Port power status	PoE status on the port: • user command set port to off: PoE to the port is turned off by the user • Standard PD was detected: A standard PD is detected • detection is in process: PDs are being detected
Port power mode	PoE mode on the port: signal: PoE through the signal cable
Port PD class	Class of power to the PD
Port power priority	PoE priority of the port: • critical: The highest • high: High • low: Low
Port max power	The maximum available power on the port
Port current power	The current power on the port
Port average power	The average power on the port
Port peak power	The peak power on the port
Port current	The current on the port
Port voltage	The voltage on the port

Display the PoE status of all ports.

```
<Sysname> display poe interface
       PORT INDEX      POWER ENABLE   MODE  PRIORITY       STATUS
```

```
GigabitEthernet1/0/1          on   enable  signal  low      Standard PD was detected
GigabitEthernet1/0/2          on   enable  signal  low      Standard PD was detected
GigabitEthernet1/0/3          off  enable  signal  low      detection is in process
GigabitEthernet1/0/4          off  enable  signal  low      detection is in process
GigabitEthernet1/0/5          off  enable  signal  low      detection is in process
GigabitEthernet1/0/6          off  enable  signal  low      detection is in process
GigabitEthernet1/0/7          off  enable  signal  low      detection is in process
GigabitEthernet1/0/8            on   enable  signal  critical Standard PD was detected
```

……

<Omitted>

Table 1-2 display poe interface command output description

Field	Description
PORT INDEX	Port index
POWER	Power status on the port: ON/OFF
ENABLE	PoE enabled/disabled status on the port
MODE	PoE mode on the port: • signal: PoE through the signal cable • spare: PoE through the spare cable
PRIORITY	PoE priority of the port: • critical: Highest • high: High • low: Low
STATUS	PoE status on the port: • user command set port to off: PoE to the port is turned off by the user • Standard PD was detected: A standard PD is detected • PD detection is in process: PDs are being detected • If the **poe enable** command is configured on a port, and the port is not connected to a standard PD (for example, a PC), “ non-standard PD connected” will be displayed.

display poe interface power

Syntax

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

View

Any view

Parameters

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

Description

Use the **display poe interface power** command to view the power information of a specific port of the switch. If the *interface-type interface-number* argument is not specified, the command displays the power information of all ports of the switch.

Examples

Display the power information of GigabitEthernet 1/0/10.

```
<Sysname> display poe interface power GigabitEthernet1/0/10
Port power                    :12400 mW
```

Display the power information of all ports.

```
<Sysname> display poe interface power
       PORT INDEX       POWER (mW)               PORT INDEX      POWER (mW)
 GigabitEthernet1/0/1           0                 GigabitEthernet1/0/2          0
 GigabitEthernet1/0/3           0                 GigabitEthernet1/0/4          0
 GigabitEthernet1/0/5           0                 GigabitEthernet1/0/6          0
 GigabitEthernet1/0/7           0                 GigabitEthernet1/0/8          0
 GigabitEthernet1/0/9           0                 GigabitEthernet1/0/10         12400
```

……

<Omitted>

display poe powersupply

Syntax

display poe powersupply

View

Any view

Parameters

None

Description

Use the **display poe powersupply** command to view the parameters of the power sourcing equipment (PSE).

Examples

Display the PSE parameters.

```
<Sysname> display poe powersupply
Unit 1
PSE ID                      :0
PSE Legacy Detection        :disable
PSE Total Power Consumption :0 mW
PSE Available Power         :300000 mW
PSE Peak Value              :0 mW
PSE Average Value           :0 mW
```

```
PSE Software Version        :290
PSE Hardware Version        :000
PSE CPLD Version            :078
PSE Power-Management mode   :auto
```

Table 1-3 display poe powersupply command output description

Field	Description
PSE ID	Identification of the PSE
PSE Legacy Detection	The enabled/disabled status of the nonstandard PD detection
PSE Total Power Consumption	Total power consumption of the PSE
PSE Available Power	Available power of the PSE
Power Peak Value	Peak power value of the PSE
Power Average Value	Average power value of the PSE
Power Software Version	Version of the PSE software
Power Hardware Version	Version of the PSE hardware
PSE CPLD Version	Version of the PSE complex programmable logical device (CPLD)
PSE Power-Management mode	PoE management mode on the port when the PSE is overloaded: • The **auto** keyword indicates that the auto mode is adopted, that is, the PoE management mode based on the PoE priority of the port is adopted • The **manual** keyword indicates that the manual mode is adopted in the PoE management on the port

display poe temperature-protection

Syntax

display poe temperature-protection

View

Any view

Parameters

None

Description

Use the **display poe temperature-protection** command to display the enable/disable status of the PoE over-temperature protection function on the switch.

Related commands: **poe temperature-protection enable**.

Examples

Display the enable/disable status of the PoE over-temperature protection function on the switch.

```
<Sysname> display poe temperature-protection
The temperature protection is enabled.
```

poe disconnect

Syntax

poe disconnect { **ac** | **dc** }

undo poe disconnect

View

System view

Parameters

ac: Specifies the PD disconnection detection mode as **ac**.

dc: Specifies the PD disconnection detection mode as **dc**.

Description

Use the **poe disconnect** command to configure a PD disconnection detection mode.

Use the **undo poe disconnect** command to restore the default.

The default PD disconnection detection mode is AC.

Note that change to the PD disconnection detection mode may lead to power-off of some PDs.

Examples

Set the PD disconnection detection mode to DC.

```
<Sysname> system-view
[Sysname] poe disconnect dc
```

poe enable

Syntax

poe enable

undo poe enable

View

Ethernet port view

Parameters

None

Description

Use the **poe enable** command to enable the PoE feature on a port.

Use the **undo poe enable** command to disable the PoE feature on a port.

By default, the PoE feature on a port is enabled by the default configuration file when the device is delivered.

If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device.

You can use the **display poe interface** command to display whether PoE is enabled on a port.

Examples

Enable the PoE feature on GigabitEthernet 1/0/3.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe enable
```

poe legacy enable

Syntax

poe legacy enable

undo poe legacy enable

View

System view

Parameters

None

Description

Use the **poe legacy enable** command to enable the PD compatibility detection function.

Use the **undo poe legacy enable** command to disable the PD compatibility detection function.

PDs compliant with IEEE 802.3af standards are called standard PDs. When the PD compatibility detection function is enabled, the switch can detect non-standard PDs.

By default, the PD compatibility detection function is disabled.

Examples

Enable the PD compatibility detection function.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] poe legacy enable
Legacy detection is enabled
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

Ethernet port view

Parameters

max-power: Maximum power distributed to the port, ranging from 1,000 to 15,400, in mW.

Description

Use the **poe max-power** command to configure the maximum power that can be supplied by the current port.

Use the **undo poe max-power** command to restore the maximum power supplied by the current port to the default value.

By default, the maximum power that a port can supply is 15400 mW.

Note that the unit of the power is mW and you can set the power in the granularity of 100 mW. The actual maximum power will be 5% larger than what you have set allowing for the effect of transient peak power.

You can use the **display poe interface** and **display poe interface power** commands to display the power supply information of a port.

Examples

Set the maximum power supplied by GigabitEthernet 1/0/3 to 15000 mW.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe max-power 15000
```

poe mode

Syntax

poe mode { **signal** | **spare** }

undo poe mode

View

Ethernet port view

Parameters

signal: Supplies power through a signal cable.

spare: Supplies power through a spare cable.

Description

Use the **poe mode** command to configure the PoE mode on the current port.

Use the **undo poe mode** command to restore the PoE mode on the current port to the default mode.

By default, **signal** mode is adopted on a port.

Note that the Switch 4200G does not support the **spare** mode currently.

Examples

Set the PoE mode on GigabitEthernet 1/0/3 to **signal**.

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

```
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe mode signal
```

poe power-management

Syntax

poe power-management { **auto | manual** }

undo poe power-management

View

System view

Parameters

auto: Adopts the **auto** mode, namely, a PoE management mode based on PoE priority of the port.

manual: Adopts the **manual** mode.

Description

Use the **poe power-management** command to configure the PoE management mode of port used in the case of power overloading.

Use the **undo poe power-management** command to restore the default mode.

By default, the PoE management mode on port is **auto**.

You can use the **poe priority** command to set the PoE priority of a port.

Examples

Configure the PoE management mode on a port to **auto**, that is, adopt the PoE management mode based on the PoE priority of the port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] poe power-management auto
Auto Power Management is enabled
```

poe priority

Syntax

poe priority { **critical** | **high | low** }

undo poe priority

View

Ethernet port view

Parameters

critical: Sets the port priority to **critical**.

high: Sets the port priority to **high**.

low: Sets the port priority to **low**.

Description

Use the **poe priority** command to configure the PoE priority of a port.

Use the **undo poe priority** command to restore the default PoE priority.

By default, the PoE priority of a port is **low**.

When the available power of the PSE is too small, the PoE priority and the PoE management mode are used together to determine how to allocate PoE power for the new PDs.

1) When the manual PoE management mode is adopted:

The switch will not supply power to the new PDs if the available power of the PSE is less than 18.8 W.

2) When the auto PoE management mode is adopted:

- If a PD is plugged into the port with a higher priority when the available power of the PSE is less than 18.8 W, the power supply to the port with the biggest number in the port group with the lowest priority is turned off, so that a part of power is released for the new PD.
- If the available power of the whole switch is less than 18.8 W and there is no port with low priority, the port with the inserted PD cannot supply power.

Examples

Set the PoE priority of GigabitEthernet 1/0/3 to **critical**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe priority critical
```

poe temperature-protection

Syntax

poe temperature-protection enable

undo poe temperature-protection enable

View

System view

Parameters

None

Description

Use the **poe temperature-protection enable** command to enable PoE over-temperature protection on the switch.

Use the **undo poe temperature-protection enable** command to disable PoE over-temperature protection on the switch.

The PoE over-temperature protection operates as follows:

The switch disables the PoE feature on all ports when its internal temperature exceeds 65°C (149°F) for self-protect, and restores the PoE feature settings on all its ports when the temperature drops below 60°C (140°F).

By default, PoE over-temperature protection is enabled on the switch.

You can use the **display poe temperature-protection** command to display whether PoE over-temperature protection is enabled on the switch.

Examples

Disable PoE over-temperature protection on the switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] undo poe temperature-protection enable
The temperature protection is disabled.
```

poe update

Syntax

poe update { **refresh** | **full** } *filename*

View

System view

Parameters

refresh: The **refresh** update mode is used when the PSE processing software is available. The **refresh** update mode is to upgrade the original processing software in the PSE.

full: The **full** update mode is used when the PSE processing software is damaged. The **full** update mode is to delete the original damaged software in the PSE completely and then reload the PoE processing software.

filename: Update file name, with a length of 1 to 64 characters and with the extension **.s19**.

Description

Use the **poe update** command to update the PSE processing software online.

Note

- Use the **full** mode only when the **refresh** mode fails. In normal cases, use the **refresh** mode.
- When the PSE processing software is damaged (that is, all the PoE commands cannot be successfully executed), you can use the **full** mode to update and restore the software.
- When the online upgrading procedure is interrupted for some unexpected reason, for example, the device is restarted due to some errors. If the upgrade in **full** mode fails after restart, you must upgrade in **full** mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.

Examples

Update the PSE processing software online.

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

```
[Sysname] poe update refresh 0400_001.S19
Update PoE board successfully
```

2 PoE Profile Configuration Commands

PoE Profile Configuration Commands

apply poe-profile

Syntax

In system view use the following commands:

apply poe-profile *profile-name* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]

undo apply poe-profile *profile-name* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]

In Ethernet port view use the following commands:

apply poe-profile *profile-name*

undo apply poe-profile *profile-name*

View

System view, Ethernet port view

Parameters

profile-name: Name of a PoE profile, a string of 1 to 15 characters. It starts with a letter from a to z or from A to Z, and it cannot be any of reserved keywords like **all**, **interface**, **user**, **undo**, and **mode**.

interface-type interface-number: Port type and port number. With this argument provided, you can specify the Ethernet port on which the existing PoE profile configuration is applied in system view.

Description

Use the **apply poe-profile** command to apply the existing PoE profile configuration to the specified Ethernet port.

Use the **undo apply poe-profile** command to cancel the PoE profile configuration for the specified Ethernet port.

Only one PoE profile can be in use at any time for each Ethernet port.

Note

PoE profile is a set of PoE configurations. One PoE profile can contain multiple PoE features. When the **apply poe-profile** command is used to apply a PoE profile to a port, some PoE features can be applied successfully while some cannot. PoE profiles are applied to Switch 4200G according to the following rules:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the **display current-configuration** command is used for query, it is displayed that the PoE profile is applied properly to the port.
- If one or more features in the PoE profile are not applied properly on a port, the switch will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
- The **display current-configuration** command can be used to query which PoE profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profile are applied successfully.

Examples

Apply the existing PoE profile (profile-test) configuration to ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/9 of the switch.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] apply poe-profile profile-test interface GigabitEthernet1/0/1 to GigabitEthernet1/0/9
```

display poe-profile

Syntax

display poe-profile { **all-profile** | **interface** *interface-type interface-number* | **name** *profile-name* }

View

Any view

Parameters

all-profile: Displays all PoE profiles.

interface-type interface-number: Port type and port number. With this argument provided, you can display the created PoE profile on a specified port.

profile-name: Name of a specified PoE profile.

Description

Use the **display poe-profile** command to display detailed configuration information of the created PoE profile for a switch.

Related commands: **poe-profile**, **apply poe-profile**.

Examples

Display detailed configuration information for the PoE profile by the name of profile-test.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] display poe-profile name profile-test
Poe-profile: profile-test, 3 action
poe enable
poe max-power 5000
poe priority critical
```

poe-profile

Syntax

poe-profile *profile-name*

undo poe-profile *profile-name*

View

System view

Parameters

profile-name: Name of PoE profile, a string of 1 to 15 characters. It starts with a letter from a to z or from A to Z, and it cannot be any of reserved keywords like **all**, **interface**, **user**, **undo**, and **mode**.

Description

Use the **poe-profile** command to create a PoE profile and then enter PoE profile view. If the PoE profile is already created, you will enter PoE profile view directly.

Use the **undo poe-profile** command to delete an existing PoE profile.

The following PoE features can be configured in the PoE profile mode:

poe enable

poe mode { **signal** | **spare** }

poe priority { **critical** | **high** | **low** }

poe max-power *max-power*

The maximum number of PoE profiles that can be configured for a Switch 4200G is 100.

Related commands: **display poe-profile**, **apply poe-profile**.

Examples

Create a PoE profile by the name of profile-test.

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

Table of Contents

1 PKI Configuration Commands

PKI Configuration Commands

attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*

undo attribute { *id* | **all** }

View

Certificate attribute group view

Parameters

id: Sequence number of the certificate attribute rule, in the range 1 to 16.

alt-subject-name: Specifies the name of the alternative certificate subject.

fqdn: Specifies the FQDN of the entity.

ip: Specifies the IP address of the entity.

issuer-name: Specifies the name of the certificate issuer.

subject-name: Specifies the name of the certificate subject.

dn: Specifies the distinguished name of the entity.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

all: Specifies all certificate attributes.

Description

Use the **attribute** command to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use the **undo attribute** command to delete the attribute rules of one or all certificates.

By default, there is no restriction on the issuer name, subject name, and alternative subject name of a certificate.

Note that the attribute of the alternative certificate subject name does not appear as a distinguished name, and therefore the **dn** keyword is not available for the attribute.

Examples

Create a certificate attribute rule, specifying that the DN in the subject name includes the string of abc.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-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-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-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

Parameters

name: Identifier of the trusted CA, a case-insensitive string of 1 to 63 characters.

Description

Use the **ca identifier** command to specify the trusted CA and bind the device with the CA.

Use the **undo ca identifier** command to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

Examples

Specify the trusted CA as **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

View

PKI domain view

Parameters

entity-name: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

Description

Use the **certificate request entity** command to specify the entity for certificate request.

Use the **undo certificate request entity** command to remove the configuration.

By default, no entity is specified for a PKI domain.

Related commands: **pki entity**.

Examples

Specify the entity for certificate request as **entity1**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request entity entity1
```

certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

View

PKI domain view

Parameters

ca: Indicates that the entity requests a certificate from a CA.

ra: Indicates that the entity requests a certificate from an RA.

Description

Use the **certificate request from** command to specify the authority for certificate request.

Use the **undo certificate request from** command to remove the configuration.

By default, no authority is specified for a PKI domain view.

Examples

Specify that the entity requests a certificate from the CA.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*]* | **manual** }

undo certificate request mode

View

PKI domain view

Parameters

auto: Specifies to request a certificate in auto mode.

key-length: Length of the RSA keys, in the range 512 to 2,048 bits. It is 1,024 bits by default.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

cipher: Specifies to display the password in cipher text.

simple: Specifies to display the password in clear text.

manual: Specifies to request a certificate in manual mode.

Description

Use the **certificate request mode** command to set the certificate request mode.

Use the **undo certificate request mode** command to restore the default.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate or when the existing certificate is about to expire. In manual mode, all operations associated with certificate request are carried out manually.

Related commands: **pki request-certificate**.

Examples

Specify to request a certificate in auto mode.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *minutes* }

undo certificate request polling { **count** | **interval** }

View

PKI domain view

Parameters

count: Maximum number of attempts to poll the status of the certificate request, in the range 1 to 100.

minutes: Polling interval, in the range 5 to 168 minutes.

Description

Use the **certificate request polling** command to specify the certificate request polling interval and attempt limit.

Use the **undo certificate request polling** command to restore the defaults.

By default, the polling is executed every 20 minutes for up to 5 times.

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related commands: **display pki certificate**.

Examples

Specify the polling interval as 15 minutes and the maximum number of attempts as 40.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

Parameters

url-string: URL of the server for certificate request, a case-insensitive string of 1 to 225 characters. It comprises the location of the server and the location of CGI command interface script in the format of *http: //server_location/ca_script_location*, where *server_location* must be an IP address and does not support domain name resolution currently.

Description

Use the **certificate request url** command to specify the URL of the server for certificate request through SCEP.

Use the **undo certificate request url** command to remove the configuration.

By default, no URL is specified for a PKI domain.

Examples

Specify the URL of the server for certificate request.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]              certificate              request              url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

Parameters

name: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **common-name** command to configure the common name of an entity, which can be, for example, the user name.

Use the **undo common-name** command to remove the configuration.

By default, no common name is specified.

Examples

Configure the common name of an entity as **test**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] common-name test
```

country

Syntax

country *country-code-str*

undo country

View

PKI entity view

Parameters

country-code-str: Country code for the entity, a 2-character case-insensitive string.

Description

Use the **country** command to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use the **undo country** command to remove the configuration.

By default, no country code is specified.

Examples

Set the country code of an entity to **CN**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

crl check

Syntax

crl check disable

undo crl check disable

View

PKI domain view

Parameters

disable: Disables CRL checking.

Description

Use the **crl check** command to disable CRL checking. Use the **undo crl check** command to restore the defaults.

By default, CRL checking is enabled.

CRLs are files issued by the CA to publish all certificates that have been revoked. Revocation of a certificate may occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

Examples

Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

crl update-period

Syntax

crl update-period *hours*

undo crl update-period

View

PKI domain view

Parameters

hours: CRL update period, in the range 1 to 720 hours.

Description

Use the **crl update-period** command to set the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs.

Use the **undo crl update-period** command to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

The CRL update period is the interval at which a PKI entity with a certificate downloads a CRL from LDAP server.

Examples

Set the CRL update period to 20 hours.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

Parameters

url-string: URL of the CRL distribution point, a case-insensitive string of 1 to 255 characters in the format of *ldap://server_location* or http://*server_location,* where *server_location* must be an IP address and does not support domain name resolution currently.

Description

Use the **crl url** command to specify the URL of the CRL distribution point.

Use the **undo crl url** command to remove the configuration.

By default, no CRL distribution point URL is specified.

Note that when the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.

Examples

Specify the URL of the CRL distribution point.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0.30
```

display pki certificate

Syntax

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** }

View

Any view

Parameters

ca: Displays the CA certificate.

local: Displays the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

request-status: Displays the status of a certificate request.

Description

Use the **display pki certificate** command to display the contents or request status of a certificate.

Related commands: **pki retrieval-certificate**, **pki domain** and **certificate request polling**.

Examples

Display the local certificate.

```
<Sysname> display pki certificate local domain 1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@aabbcc.net
            C=CN
            ST=Country A
            L=City X
            O=abc
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2004 GMT
            Not After : Jan 20 09:07:21 2005 GMT
        Subject:
            C=CN
            ST=Country B
            L=City Y
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00D41D1F …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS: hyf.xxyyzz.net
            X509v3 CRL Distribution Points:
            URI:http://1.1.1.1:447/myca.crl
```

```
            …              …
    Signature Algorithm: md5WithRSAEncryption
        A3A5A447 4D08387D …
```

Table 1-1 display pki certificate command output description

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of the X.509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X.509 (version 3) CRLs

display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy { *policy-name* | **all** }

View

Any view

Parameters

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

all: Specifies all certificate attribute-based access control policies.

Description

Use the **display pki certificate access-control-policy** command to display information about a specified or all certificate attribute-based access control policies.

Examples

Display information about the certificate attribute-based access control policy named mypolicy.

```
<Sysname> display pki certificate access-control-policy mypolicy
 access-control-policy name: mypolicy
     rule  1 deny    mygroup1
     rule  2 permit  mygroup2
```

Table 1-2 display pki certificate access-control-policy command output description

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy

Field	Description
rule number	Number of the access control rule

display pki certificate attribute-group

Syntax

display pki certificate attribute-group { *group-name* | **all** }

View

Any view

Parameters

group-name: Name of a certificate attribute group, a string of 1 to 16 characters.

all: Specifies all certificate attribute groups.

Description

Use the **display pki certificate attribute-group** command to display information about a specified or all certificate attribute groups.

Examples

Display information about certificate attribute group mygroup.

```
<Sysname> display pki certificate attribute-group mygroup
 attribute group name: mygroup
      attribute  1 subject-name     dn    ctn   abc
      attribute  2 issuer-name      fqdn  nctn  app
```

Table 1-3 display pki certificate attribute-group command output description

Field	Description
attribute group name	Name of the certificate attribute group
attribute *number*	Number of the attribute rule
subject-name	Name of the certificate subject
dn	DN of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

display pki crl domain

Syntax

display pki crl domain *domain-name*

View

Any view

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use the **display pki crl domain** command to display the locally saved CRLs.

Related commands: **pki retrieval-crl**, **pki domain**.

Examples

Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=CN
            O=abc
            OU=soft
            CN=A Test Root
        Last Update: Jan  5 08:44:19 2004 GMT
        Next Update: Jan  5 21:42:13 2004 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
            Revoked Certificates:
            Serial Number: 05a234448E…
            Revocation Date: Sep 6 12:33:22 2004 GMT
            CRL entry extensions:…
            Serial Number: 05a278445E…
            Revocation Date: Sep 7 12:33:22 2004 GMT
            CRL entry extensions:…
```

Table 1-4 display pki crl domain command output description

Field	Description
Version	Version of the CRLs
Signature Algorithm	Signature algorithm used by the CRLs
Issuer	CA issuing the CRLs
Last Update	Last update time

Field	Description
Next Update	Next update time
CRL extensions	Extensions of CRL
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X.509v3.
keyid	ID of the public key A CA may have multiple key pairs. This field indicates the key pair used by the CRL's signature.
Revoked Certificates	Revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Revocation date of the certificate

fqdn

Syntax

fqdn *name-str*

undo fqdn

View

PKI entity view

Parameters

name-str: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 255 characters.

Description

Use the **fqdn** command to configure the FQDN of an entity.

Use the **undo fqdn** command to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

Examples

Configure the FQDN of an entity as **pki.domain-name.com**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

ip (PKI entity view)

Syntax

ip *ip-address*

undo ip

View

PKI entity view

Parameters

ip-address: IP address for an entity.

Description

Use the **ip** command to configure the IP address of an entity.

Use the **undo ip** command to remove the configuration.

By default, no IP address is specified for an entity.

Examples

Configure the IP address of an entity as 11.0.0.1.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

ldap-server

Syntax

ldap-server ip *ip-address* [**port** *port-number*] [**version** *version-number*]

undo ldap-server

View

PKI domain view

Parameters

ip-address: IP address of the LDAP server, in dotted decimal format.

port-number: Port number of the LDAP server, in the range 1 to 65535. The default is 389.

version-number: LDAP version number, either 2 or 3. By default, it is 2.

Description

Use the **ldap-server** command to specify an LDAP server for a PKI domain.

Use the **undo ldap-server** command to remove the configuration.

By default, no LDP server is specified for a PKI domain.

Examples

Specify an LDAP server for PKI domain 1.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

locality

Syntax

locality *locality-name*

undo locality

View

PKI entity view

Parameters

locality-name: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **locality** command to configure the geographical locality of an entity, which can be, for example, a city name.

Use the **undo locality** command to remove the configuration.

By default, no geographical locality is specified for an entity.

Examples

Configure the locality of an entity as **city**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

organization

Syntax

organization *org-name*

undo organization

View

PKI entity view

Parameters

org-name: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **organization** command to configure the name of the organization to which the entity belongs.

Use the **undo organization** command to remove the configuration.

By default, no organization name is specified for an entity.

Examples

Configure the name of the organization to which an entity belongs as **org-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization org-name
```

organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

View

PKI entity view

Parameters

org-unit-name: Organization unit name for distinguishing different units in an organization, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **organization-unit** command to specify the name of the organization unit to which this entity belongs.

Use the **undo organization-unit** command to remove the configuration.

By default, no organization unit name is specified for an entity.

Examples

Configure the name of the organization unit to which an entity belongs as **unit-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit unit-name
```

pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

View

System view

Parameters

policy-name: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be “a”, “al” or “all”.

all: Specifies all certificate attribute-based access control policies.

Description

Use the **pki certificate access-control-policy** command to create a certificate attribute-based access control policy and enter its view.

Use the **undo pki certificate access-control-policy** command to remove a specified or all certificate attribute-based access control policies.

No access control policy exists by default.

Examples

Configure an access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

View

System view

Parameters

group-name: Name for the certificate attribute group, a case-insensitive string of 1 to 16 character.

all: Specifies all certificate attribute groups.

Description

Use the **pki certificate attribute-group** command to create a certificate attribute group and enter its view.

Use the **undo pki certificate attribute-group** command to delete one or all certificate attribute groups.

By default, no certificate attribute group exists.

Examples

Create a certificate attribute group named **mygroup** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

pki delete-certificate

Syntax

pki delete-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Parameters

ca: Deletes the locally stored CA certificate.

local: Deletes the locally stored local certificate.

domain-name: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

Description

Use the **pki delete-certificate** command to delete the certificate locally stored for a PKI domain.

Examples

Delete the local certificate for PKI domain cer.

```
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

Parameters

domain-name: PKI domain name, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki domain** command to create a PKI domain and enter PKI domain view or enter the view of an existing PKI domain.

Use the **undo pki domain** command to remove a PKI domain.

By default, no PKI domain exists.

Examples

Create a PKI domain and enter its view.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

Parameters

entity-name: Name for the entity, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki entity** command to create a PKI entity and enter PKI entity view.

Use the **undo pki entity** command to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

Examples

Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

pki import-certificate

Syntax

pki import-certificate { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

View

System view

Parameters

ca: Specifies the CA certificate.

local: Specifies the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

der: Specifies the certificate format of DER.

p12: Specifies the certificate format of P12.

pem: Specifies the certificate format of PEM.

filename: Name of the certificate file, a case-insensitive string of 1 to 127 characters. It defaults to *domain-name*_ca.cer, *domain-name*_local.cer, or *domain-name*_peerentity_*entity-name*.cer, the name for the file to be created to save the imported certificate.

Description

Use the **pki import-certificate** command to import a CA certificate or local certificate from a file and save it locally.

Related commands: **pki domain**.

Examples

Import the CA certificate for PKI domain cer in the format of PEM.

```
<Sysname> system-view
[Sysname] pki import-certificate ca domain cer pem
```

pki request-certificate domain

Syntax

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

View

System view

Parameters

domain-name: Name of the PKI domain name, a string of 1 to 15 characters.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

pkcs10: Displays the BASE64-encoded PKCS#10 certificate request.

filename: Name of the file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

Description

Use the **pki request-certificate domain** command to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to save the local certificate request in BASE64 format and send it to the CA by an out-of-band means like phone, disk or e-mail.

This operation will not be saved in the configuration file.

Related commands: **pki domain**.

Examples

Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
```

pki retrieval-certificate

Syntax

pki retrieval-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Parameters

ca: Retrieves the CA certificate.

local: Retrieves the local certificate.

domain-name: Name of the PKI domain used for certificate request.

Description

Use the **pki retrieval-certificate** command to retrieve a certificate from the server for certificate distribution.

Related commands: **pki domain**.

Examples

Retrieve the CA certificate from the certificate issuing server.

```
<Sysname> system-view
[Sysname] pki retrieval-certificate ca domain 1
```

pki retrieval-crl domain

Syntax

pki retrieval-crl domain *domain-name*

View

System view

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use the **pki retrieval-crl** command to retrieve the latest CRLs from the server for CRL distribution.

CRLs are used to verify the validity of certificates.

Related commands: **pki domain**.

Examples

Retrieve CRLs.

```
<Sysname> system-view
[Sysname] pki retrieval-crl domain 1
```

pki validate-certificate

Syntax

pki validate-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Parameters

ca: Verifies the CA certificate.

local: Verifies the local certificate.

domain-name: Name of the PKI domain to which the certificate to be verified belongs, a string of 1 to 15 characters.

Description

Use the **pki validate-certificate** command to verify the validity of a certificate.

The focus of certificate validity verification is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related commands: **pki domain**.

Examples

Verify the validity of the local certificate.

```
<Sysname> system-view
[Sysname] pki validate-certificate local domain 1
```

root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

View

PKI domain view

Parameters

md5: Uses an MD5 fingerprint.

sha1: Uses a SHA1 fingerprint.

string: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

Description

Use the **root-certificate fingerprint** command to configure the fingerprint to be used for verifying the validity of the CA root certificate.

Use the **undo root-certificate fingerprint** command to remove the configuration.

By default, no fingerprint is configured for verifying the validity of the CA root certificate.

Examples

Configure an MD5 fingerprint for verifying the validity of the CA root certificate.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

Configure a SHA1 fingerprint for verifying the validity of the CA root certificate.

```
[Sysname-pki-domain-1]           root-certificate           fingerprint           sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

rule (access control policy view)

Syntax

rule [*id*] { **deny** | **permit** } *group-name*

undo rule { *id* | **all** }

View

Access control policy view

Parameters

id: Number of the certificate attribute access control rule, in the range 1 to 16. The default is the smallest unused number in this range.

deny: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered invalid and denied.

permit: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered valid and permitted.

group-name: Name of the certificate attribute group to be associated with the rule.

all: Specifies all access control rules.

Description

Use the **rule** command to create a certificate attribute access control rule.

Use the **undo rule** command to delete a specified or all access control rules.

By default, no access control rule exists.

Note that a certificate attribute group must exist to be associated with a rule.

Examples

Create an access control rule, specifying that a certificate is considered valid when it matches an attribute rule in certificate attribute group mygroup.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

state

Syntax

state *state-name*

undo state

View

PKI entity view

Parameters

state-name: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **state** command to specify the name of the state or province where an entity resides.

Use the **undo state** command to remove the configuration.

By default, no state or province is specified.

Examples

Specify the state where an entity resides.

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

```
[Sysname] pki entity 1
[Sysname-pki-entity-1] state country
```

Table of Contents

1 SSL Configuration Commands

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

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 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 the **ciphersuite** command to specify the cipher suite(s) for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.

Examples

Specify the cipher suites for SSL server policy policy1 to support as **rsa_rc4_128_md5** and **rsa_rc4_128_sha**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

client-verify enable

Syntax

client-verify enable

undo client-verify enable

View

SSL server policy view

Parameters

None

Description

Use the **client-verify enable** command to enable certificate-based SSL client authentication, that is, to enable the SSL server to perform certificate-based authentication of the client during the SSL handshake process.

Use the **undo client-verify enable** command to restore the default.

By default, certificate-based SSL client authentication is disabled.

Examples

Enable certificate-based client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

close-mode wait

Syntax

close-mode wait

undo close-mode wait

View

SSL server policy view

Parameters

None

Description

Use the **close-mode wait** command to set the SSL connection close mode to wait. In this mode, after sending a close-notify message to a client, the server does not close the connection until it receives a close-notify message from the client.

Use the **undo close-mode wait** command to restore the default.

By default, an SSL server sends a close-notify alert message to the client and close the connection without waiting for the close-notify alert message from the client.

Examples

Set the SSL connection close mode to wait mode.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

display ssl server-policy

Syntax

display ssl server-policy { *policy-name* | **all** }

View

Any view

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 255 characters.

all: Displays information about all SSL server policies.

Description

Use the **display ssl server-policy** command to view information about a specified or all SSL server policies.

Examples

Display information about SSL server policy policy1.

```
<Sysname> display ssl server-policy policy1
ssl-policy: policy1
         pki-domain:
         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: enabled
```

Table 1-1 display ssl server-policy command output description

Field	Description
ssl-policy	SSL server policy name
pki-domain	PKI domain used by the SSL server policy
ciphersuite	Cipher suite supported by the SSL server policy

Field	Description
handshake timeout	Handshake timeout time of the SSL server policy, in seconds
close-mode	Close mode of the SSL server policy
session timeout	Session timeout time of the SSL server policy, in seconds
session cachesize	Maximum number of buffered sessions of the SSL server policy
client-verify	Whether client authentication is enabled

handshake timeout

Syntax

handshake timeout *time*

undo handshake timeout

View

SSL server policy view

Parameters

time: Handshake timeout time in seconds, in the range 180 to 7,200.

Description

Use the **handshake timeout** command to set the handshake timeout time for an SSL server policy.

Use the **undo handshake timeout** command to restore the default.

By default, the handshake timeout time is 3,600 seconds.

If the SSL server does not receive any packet from the SSL client before the handshake timeout time expires, the SSL server will terminate the handshake process.

Examples

Set the handshake timeout time of SSL server policy policy1 to 3,000 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view

Parameters

domain-name: Name of a PKI domain, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki-domain** command to specify a PKI domain for an SSL server policy.

Use the **undo pki-domain** command to restore the default.

By default, no PKI domain is configured for an SSL server policy.

Examples

Configure SSL server policy policy1 to use the PKI domain named server-domain.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

session

Syntax

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

View

SSL server policy view

Parameters

size: Maximum number of cached sessions, in the range 100 to 1,000.

time: Caching timeout time in seconds, in the range 1,800 to 72,000.

Description

Use the **session** command to set the maximum number of cached sessions and the caching timeout time.

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

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3,600 seconds.

The process of the session parameters negotiation and session establishment by using the SSL handshake protocol is quite complicated. SSL allows reusing the negotiated session parameters to establish sessions. Therefore, the SSL server needs to maintain information about existing sessions. Note that the number of sessions and the time that the session information will be maintained are limited:

- If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions.
- If a session exists in the cache for a period equal to the caching timeout time, SSL will remove the information of the session.

Examples

Set the caching timeout time to 4,000 seconds and the maximum number of cached sessions to 600.

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

```
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View

System view

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be “a”, “al” and “all”.

all: Specifies all SSL server policies.

Description

Use the **ssl server-policy** command to create an SSL server policy and enter its view.

Use the **undo ssl server-policy** command to remove a specified or all SSL server policies.

Note that you cannot delete an SSL server policy that has been associated with one or more application layer protocols.

Examples

Create an SSL server policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

Table of Contents

1 Web Authentication Configuration Commands

Web Authentication Configuration Commands

display web-authentication configuration

Syntax

display web-authentication configuration

View

Any view

Parameters

None

Description

Use the **display web-authentication configuration** command to display all Web authentication configurations, including global configurations and configurations on individual ports.

Examples

Display Web authentication configuration information.

```
<Sysname> display web-authentication configuration
Status: enabled
     Web Server: IP=30.1.1.2        Port=80
     Idle-cut time: 900 sec
     Max-online time: 1800 sec
     Max-connection of device is: 512
Customized authentication-page information :
     Corp-Name: 3Com Corporation
     Platform-Name: A leading global supplier of IP-based products and solutions
     Phone-Num: 1-800-876-3266
     Email-address: relations@3com.com
     File:
Free IP:
           1) IP=10.1.1.0           Net Mask=255.255.255.0
 Free User:
           1) IP=192.168.0.108      MAC=000d-88f6-44c1
 Interface Configuration:
 Interface_number         method        max-connection
 GigabitEthernet1/0/1            shared        128
 GigabitEthernet1/0/14           shared        128
```

Table 1-1 Description on the fields of display web-authentication configuration

Field	Description
Status	Global status of Web authentication
Web Server	IP address and port number of the Web authentication server
Idle-cut time	idle user checking interval
Max-online time	Maximum online time specified for Web authentication users
Max-connection of device	Maximum number of Web authentication users allowed on the device
Customized authentication-page information	Customized information to be displayed on authentication pages, including company name, subject, contact phone number, and E-mail address.
Free IP	Free IP address range information
Free User	Authentication-free user information
Interface Configuration	Configuration information about Web-authentication-enabled ports
Interface_number	Index of a Web-authentication-enabled port
method	User access method on the port, Shared or Designated.
max-connection	Maximum number of online users allowed on the port

display web-authentication connection

Syntax

display web-authentication connection { **all** | **interface** *interface-type interface-number* | **user-name** *user-name* }

View

Any view

Parameters

all: Displays information about all online Web-authentication users.

interface-type interface-number: Type and number of an interface.

user-name: Name of a user, a string of 1 to 184 characters.

Description

Use the **display web-authentication connection** command to display information about specified or all online Web-authentication users.

Examples

Display information about all online Web-authentication users.

```
<Sysname> display web-authentication connection all
Username: 1
MAC: 000d-88f6-44c1   Interface: GigabitEthernet1/0/1
VLAN: 2               Method: Shared
State: ONLINE         Online-Time(s): 8

Total 1 connection(s) matched
```

Table 1-2 Description on the fields of **display web-authentication connection**

Field	Description
Username	Name of an online Web-authentication user
MAC	MAC address of the user
Interface	Access port of the user
VLAN	VLAN the user belongs to
Method	Access method of the user, Shared or Designated.
State	User status
Online-Time(s)	Online time of the user

web-authentication customize

Syntax

web-authentication customize { **corp-name** *corporation-text* | **email** *email-string* | **phone-num** *phonenum-string* | **platform-name** *platform-text* | **file** *web-file* }

undo web-authentication customize { **corp-name** | **email** | **phone-num** | **platform-name** | **file** | **all** }

View

System view

Parameters

corp-name: Specifies the company name to be displayed on Web authentication pages.

corporation-text: Company name, a string of 1 to 64 characters that can contain spaces.

email: Specifies the E-mail address to be displayed on Web authentication pages.

email-string: E-mail address, a string of 1 to 64 characters that can contain spaces. If it contains spaces, it must be enclosed with a pair of double quotation marks.

phone-num: Specifies the phone number to be displayed on Web authentication pages.

phonenum-string: Phone number, a string of 1 to 32 characters that can contain spaces. If it contains spaces, it must be enclosed with a pair of double quotation marks.

platform-name: Specifies the subject to be displayed on Web authentication pages.

platform-text: Subject introduction, a string of 1 to 128 characters that can contain spaces.

file: Specifies the custom web file.

web-file: Specifies the name of a web file with a string of 1 to 142 letters.

all: Restores all customized items to the defaults.

Description

Use the **web-authentication customize** command to customize the company name, subject, contact phone number, and E-mail address to be displayed on authentication pages or to specify the custom web file. After the configuration, the customized information will be displayed on all Web pages provided during the authentication process.

Use the **undo web-authentication customize** command to restore the specified or all customized items to the defaults.

By default, no customized information is configured to be displayed on Web authentication pages.

Examples

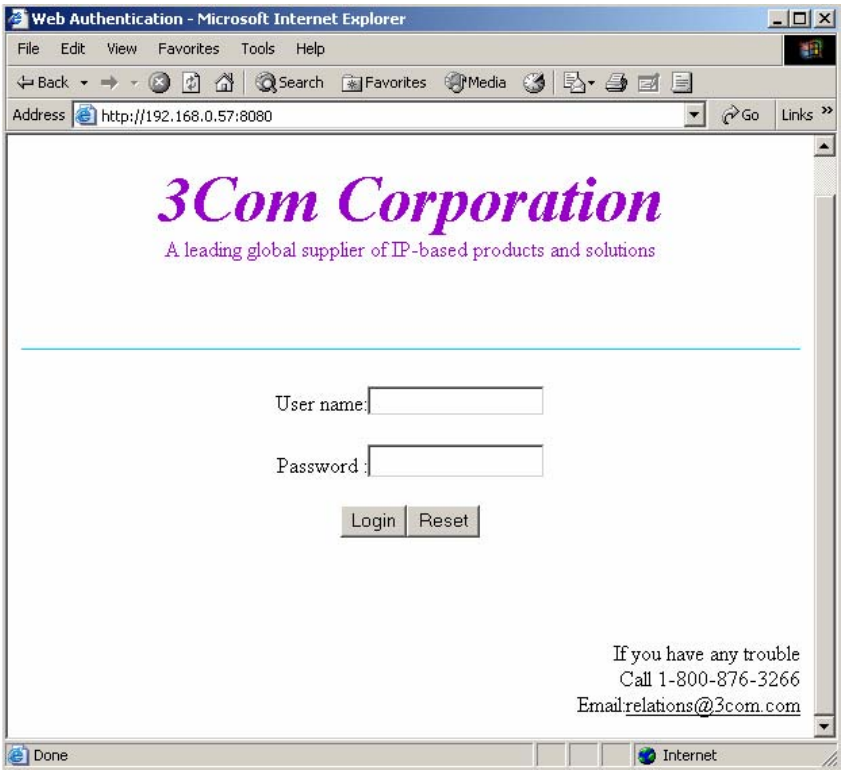
Customize information to be displayed on Web authentication pages as follows:

- Company name: 3Com Corporation
- E-mail: relations@3com.com
- Phone number: 1-800-876-3266
- Subject: A leading global supplier of IP-based products and solutions

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication customize corp-name 3Com Corporation
[Sysname] web-authentication customize email relations@3com.com
[Sysname] web-authentication customize phone-num 1-800-876-3266
[Sysname] web-authentication customize platform-name A leading global supplier of IP-based
products and solutions
```

After the above configuration, the customized information will be displayed on the Web authentication page, as shown in Figure 1-1.

Figure 1-1 Web authentication page with customized information



web-authentication cut connection

Syntax

web-authentication cut connection { **all** | **mac** *mac-address* | **user-name** *user-name* | **interface** *interface-type interface-number* }

View

System view

Parameters

all: Specifies all online users.

mac *mac-address*: Specifies an user by the user's MAC address.

user-name *user-name*: Specifies a user by the user's name, which is a string of 1 to 184 characters.

interface-type interface-number: Specifies all users on a port.

Description

Use the **web-authentication cut connection** command to forcibly log out the specified or all users.

Examples

Forcibly log out all online users on GigabitEthernet 1/0/2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication cut connection interface GigabitEthernet1/0/2
```

web-authentication enable

Syntax

web-authentication enable

undo web-authentication enable

View

System view

Parameters

None

Description

Use the **web-authentication enable** command to enable Web authentication globally.

Use the **undo web-authentication enable** command to disable Web authentication globally.

 **Note**

Web authentication cannot be enabled when one of the following features is enabled, and vice versa: 802.1x, MAC authentication, port security and port aggregation.

Examples

Enable Web authentication globally.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication web-server ip 192.168.0.56 port 80
[Sysname] web-authentication enable
```

web-authentication free-ip

Syntax

web-authentication free-ip *ip-address* { *mask-length* | *mask* }

undo web-authentication free-ip { ip-address { *mask-length* | *mask* } | **all** }

View

System view

Parameters

ip-address: IP address.

mask-length: Mask length, ranging from 1 to 32.

mask: Mask address.

Description

Use the **web-authentication free-ip** command to set a free IP address range, which can be accessed by users before they pass Web authentication.

Use the **undo web-authentication free-ip** command to remove the setting or all such settings.

By default, no free IP address range is set.

🕮 **Note:**

- The to-be-set free IP address range cannot include the Web authentication server's IP address.
- At most four free IP address range can be set.

Examples

Set IP address range 10.1.1.0/24 as a free address range.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication free-ip 10.1.1.0 24
```

web-authentication free-user

Syntax

web-authentication free-user ip *ip-address* **mac** *mac-address*

undo web-authentication free-user { **ip** *ip-address* **mac** *mac-address* | **all** }

View

System view

Parameters

ip-address: IP address of a user.

mac-address: MAC address of the user, in the format of H-H-H (for example, 000d-88f6-44c1).

all: Deletes all authentication-free user settings.

Description

Use the **web-authentication free-user** command to set an authentication-free user, so that a user whose source IP and MAC addresses are both identical with those of the authentication-free user can access the network without the necessary to pass the Web authentication.

Use the **undo web-authentication free-user** command to remove the setting or all such settings.

By default, no authentication-free user is set.

🕮 **Note:**

- You can set up to eight authentication-free users.
- After a user gets online in shared access method, if you configure an authentication-free user whose IP address and MAC address are the same as those of the online user, the online user will be forced to get offline.

Examples

Set the user with IP address 192.168.0.108 and MAC address 0010-0020-0030 as an authentication-free user.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication free-user ip 192.168.0.108 mac 0010-0020-0030
```

web-authentication max-connection

Syntax

web-authentication max-connection *number*

undo web-authentication max-connection

View

System view, port view

Parameters

number: Maximum number of online Web-authentication users on the port, in the range of 1 to 128.

Description

Use the **web-authentication max-connection** command to set the maximum number of online Web authentication users on the device or on the current port. When this threshold is reached, no more users can pass the Web authentication on the device or port.

If configured in port view, this command can be configured on only the ports that can service multiple users at a time.

By default, a port allows up to 128 online Web-authentication users, and a device allows up to 512 online Web-authentication users.

Examples

Configure GigabitEthernet 1/0/1 to allow at most 100 online Web-authentication users.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-authentication select method shared
[Sysname-GigabitEthernet1/0/1] web-authentication max-connection 100
```

web-authentication protocol

Syntax

web-authentication protocol { **http** | **https server-policy** *policy-name* }

undo web-authentication protocol

View

System view

Parameters

http: Specifies that clients use HTTP to access the authentication pages. Authentication information is not encrypted in this mode.

https: Specifies that clients use HTTPS to access the authentication pages. Authentication information is encrypted in this mode.

policy-name: Specifies the SSL server policy by its name, a string of 1 to 16 characters.

Description

Use the **web-authentication protocol** command to specify the access protocol for Web authentication. If you specify the access protocol as HTTPS, authentication information exchanged between the switch and its clients will be in ciphertext.

Use the **undo web-authentication protocol** command to restore the default.

By default, HTTP is used between the switch and its clients.

Note that:

- You must configure this command before enabling Web authentication. That is, after enabling Web authentication, you cannot change the access protocol for Web authentication.
- Before configuring HTTPS access for Web authentication, be sure to configure the SSL server policy and request a certificate for the PKI domain of the SSL server policy.
- After modifying the used SSL server policy, you need to disable Web authentication and then enable it again in system view to make the changes take effect.
- Only SSL 3.0 and TLS 1.0 are supported. SSL 2.0 is not supported.
- With HTTPS access for Web authentication configured on the switch, clients need to use HTTP 1.1 to log in. Otherwise, the speed of opening the authentication page will be very low.

Examples

Configure HTTPS access for Web authentication, specifying to use SSL server policy **pt_ssl**.

```
<Sysname> system-view
[Sysname] web-authentication protocol https server-policy pt_ssl
```

web-authentication select method

Syntax

web-authentication select method { **shared** | **designated** }

undo web-authentication select

View

Port view

Parameters

shared: Sets the Web authentication access method on the port to shared.

designated: Sets the Web authentication access method on the port to designated.

Description

Use the **web-authentication select** command to enable Web authentication on the current port and set the Web authentication access method on the port.

Use the **undo web-authentication select** command to disable Web authentication on the port.

There are two Web authentication access methods:

- shared: In this mode, the port allows multiple Web authentication users to be online at the same time.
- designated: In this mode, the port allows only one Web authentication user to be online at a time.

This configuration takes effect only when Web authentication is enabled globally. If Web authentication is not enabled globally, this configuration will only be saved.

Note:

You are not allowed to enable Web authentication on a port if:

- The port is an access port, or,
- The port belongs to an aggregation group.

Examples

Enable Web authentication on GigabitEthernet 1/0/1 and set the Web authentication access method to shared.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-authentication select method shared
```

web-authentication timer idle-cut

Syntax

web-authentication timer idle-cut *timer*

undo web-authentication timer idle-cut

View

System view

Parameters

timer: Interval for checking whether an online user is idle. It ranges from 10 to 86400 seconds. Value 0 means the idle user checking function is disabled.

Description

Use the **web-authentication timer idle-cut** command to set the idle user checking interval for Web authentication.

Use the **undo web-authentication timer idle-cut** command to restore the default.

By default, the idle user checking interval is 900 seconds for Web authentication.

 **Note**

The idle user checking interval is the interval at which the system checks whether a user is idle. When a user is found idle, if the corresponding MAC address entry has not been aged out, the system keeps the user online; otherwise, the system logs off the user. You are recommended to set the interval to a value that is greater than half of the MAC address entry aging time but less than the MAC address entry aging time.

Examples

Set the idle user checking interval to 500 seconds for Web authentication.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication timer idle-cut 500
```

web-authentication timer max-online

Syntax

web-authentication timer max-online *timer*

undo web-authentication timer max-online

View

System view

Parameters

Timer: Maximum online time specified for online users, in the range of 10 to 86400, in seconds. Value 0 means there is no limit to the online time of users.

Description

Use the **web-authentication timer max-online** command to set the maximum online time for online users. If a user does not log off after the online timer expires, the switch will log off the user forcibly.

Use the **undo web-authentication timer max-online** command to restore the default.

By default, the maximum online time for users is 1800 seconds.

Examples

Set the maximum online time of users to 36000 seconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication timer max-online 36000
```

web-authentication web-server

Syntax

web-authentication web-server ip *ip-address* [**port** *port-number*]

undo web-authentication web-server

View

System view

Parameters

ip-address: IP address of the Web authentication server. It must be a valid unicast address.

port-number: Port number of the Web authentication server. It ranges from 1 to 50000, with 80 as the default.

Description

Use the **web-authentication web-server ip** command to set the IP address and port number of the Web authentication server, which will be used for Web authentication of users.

Use the **undo web-authentication web-server** command to restore the default.

By default, no Web authentication server IP address is set and the port number is 80.

Note

Before enabling Web authentication globally, you should first set the IP address of the Web authentication server.

Examples

Set the IP address and port number of the Web authentication server to 192.168.0.56 and 80.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] web-authentication web-server ip 192.168.0.56 port 80
```

Table of Contents

1 LLDP Configuration Commands

LLDP Configuration Commands

display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

Any view

Parameters

global: Displays the global LLDP information.

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

Description

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

If no keyword or argument is specified, this command displays all the LLDP information to be sent, including the global LLDP information and the LLDP information about the LLDP-enabled ports.

Examples

Display all the LLDP information to be sent.

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID         : 00e0-fc00-5500
  System name        : Sysname
  System description : Sysname Switch
  System capabilities supported : Bridge
  System capabilities enabled   : Bridge

  MED information
  Device class: Connectivity device

  HardwareRev               : REV.A
  FirmwareRev               : 109
  SoftwareRev               : 5.20 Alpha 2101
  SerialNum                 : Unknown
  Manufacturer name         : Unknown
  Model name                : model
  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                : 192.168.102.11
  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)

  PoE supported: No

  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
```

Table 1-1 display lldp local-information command output description

Field	Description
Global LLDP local-information	The global LLDP information
Chassis ID	Device MAC address
System name	System name of the device
System description	System description

Field	Description
System capabilities supported	Supported capabilities, which can be: • Bridge, indicating switching • Router, indicating routing • Repeater, indicating forwarding
System capabilities enabled	Currently enabled capabilities, which can be: • Bridge, indicating switching is currently enabled. • Router, indicating routing is currently enabled. • Repeater, indicating forwarding is currently enabled.
PoE device type	PoE device type
MED information	MED information
Device class	MED device type
(MED inventory information of master board)	MED inventory information of the master board
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNumber	Serial number
Manufacturer name	Device manufacturer
Model name	Device model
Asset tracking identifier	Asset tracking ID
LLDP local-information of port number *interface-type interface-number*	LLDP information about a port
Port ID subtype	Port ID type
Port ID	Port ID
Port description	Port description
Management address type	Management address type
Management address	Management address
Management address interface type	Type of the interface identified by the management address
Management address interface ID	ID of the interface identified by the management address
Management address OID	Management address object ID
Port VLAN ID(PVID)	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN ID	Name of the VLAN identified by the VLAN ID
Auto-negotiation supported	Indicates whether auto-negotiation is supported on the port.
Auto-negotiation enabled	State of auto-negotiation

Field	Description
OperMau	Current speed and duplex state of the port
Power port class	PoE device type, which can be : • PSE, indicating a power supply device • PD, indicating a powered device
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be **Signal** or **Spare**.
Port power classification	Port power classification of the PD, which can be: • Class0 • Class1 • Class2 • Class3 • Class4
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
MED information	MED LLDP information
Media policy type	Media policy type, which can be: • Voice, indicating the device is capable of processing voice data. • Unknown, indicating the media policy is unknown.
Unknown Policy	Indicates whether or not the media policy is unknown.
VLAN tagged	Indicates whether packets of the voice VLAN are tagged.
Media Policy VlanID	ID of the voice VLAN
Media Policy L2 priority	Layer 2 priority
Media Policy Dscp	DSCP precedence
Location format	Location format, which can be: • Civic Address LCI, indicating normal address information. • ECS ELIN, indicating telephone number for urgencies.
Location Information	Location information
PoE PSE power source	PSE type, which can be: • Primary, indicating a primary power supply • Backup, indicating a backup power supply

Field	Description
Port PSE Priority	Port PSE priority, which can be : • Unknown • Critical • High • Low
Port Available power value	PoE power

display lldp neighbor-information

Syntax

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

View

Any view

Parameters

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

brief: Displays the LLDP information in brief.

Description

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

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

Examples

Display the LLDP information received through all the ports.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 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        : Sysname
  System description : Sysname Switch
  System capabilities supported : Repeater,Bridge,Router
  System capabilities enabled   : Repeater,Bridge,Router

  Management address type           : ipV4
  Management address                : 127.0.0.1
  Management address interface type : IfIndex
```

```
Management address interface ID   : Unknown
Management address OID            : 0

Port VLAN ID(PVID): 1

Port and protocol VLAN ID(PPVID) : 1
Port and protocol VLAN supported : Yes
Port and protocol VLAN enabled   : No

VLAN name of VLAN 1: VLAN 0001

Auto-negotiation supported : Yes
Auto-negotiation enabled   : Yes
OperMau                    : speed(1000)/duplex(Full)

Power port class          : PD
PSE power supported       : No
PSE power enabled         : No
PSE pairs control ability : No
Power pairs               : Signal
Port power classification : Class 0

Link aggregation supported : Yes
Link aggregation enabled   : No
Aggregation port ID        : 0

Maximum frame Size: 1536

Neighbor index   : 2
Update time      : 0 days,0 hours,1 minutes,1 seconds
Chassis type     : MAC address
Chassis ID       : 000f-0055-0002
Port ID type     : Interface name
Port ID          : GigabitEthernet1/0/2
Port description : GigabitEthernet1/0/2 Interface
System name        : Sysname
System description : Sysname Switch
System capabilities supported : Repeater,Bridge,Router
System capabilities enabled   : Repeater,Bridge,Router

Management address type           : ipV4
Management address                : 127.0.0.1
Management address interface type : IfIndex
Management address interface ID   : Unknown
Management address OID            : 0

Port VLAN ID(PVID): 1
```

```
Port and protocol VLAN ID(PPVID) : 1
Port and protocol VLAN supported : Yes
Port and protocol VLAN enabled   : No

VLAN name of VLAN 1: VLAN 0001

Auto-negotiation supported : Yes
Auto-negotiation enabled   : Yes
OperMau                    : speed(1000)/duplex(Full)

Power port class           : PD
PSE power supported        : No
PSE power enabled          : No
PSE pairs control ability : No
Power pairs                : Signal
Port power classification : Class 0

Link aggregation supported : Yes
Link aggregation enabled   : No
Aggregation port ID        : 0

Maximum frame Size: 1536
```

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

Field	Description
LLDP neighbor-information	LLDP information about a neighboring device
LLDP neighbor-information of Port number *interface-type interface number*	LLDP information received through a specific port
Neighbor index	Neighbor index
Update time	Time when the LLDP information about a neighboring device is latest updated.
Chassis type	Chassis information, which can be: • Chassis component • Interface alias • Port component • MAC address • Network address • Interface name • Locally assigned (indicating the local configuration)
Chassis ID	Value of chassis type

Field	Description
Port ID type	Port information, which can be: • Interface alias • Port component • MAC address • Network Address • Interface name • Agent circuit ID • Locally assigned (indicating the local configuration)
Port ID	Value of port ID type
Port description	Port description
System name	System name of the neighboring device
System description	System description of the neighboring device
System capabilities supported	Capabilities supported on the neighboring device, which can be: • Bridge, indicating switching • Router, indicating routing • Repeater, indicating forwarding
System capabilities enabled	Capabilities currently enabled on the neighboring device, which can be: • Bridge, indicating switching is currently enabled. • Router, indicating routing is currently enabled. • Repeater, indicating forwarding is currently enabled.
Management address type	Management address type
Management address	Management address
Management address interface type	Type of the interface identified by the management address
Management address interface ID	Management address interface ID
Management address OID	Management address object ID
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled.
VLAN name of VLAN 1	Name of he port VLAN
Auto-negotiation supported	Indicates whether auto-negotiation is supported.
Auto-negotiation enabled	State of auto-negotiation
OperMau	Current speed and duplex state
Power port class	PoE device type, which can be: • PSE, indicating a power supply device. • PD, indicating a powered device.
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.

Field	Description
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be **Signal** or **Spare**.
Port power classification	Port power classification of the PD, which can be the following: • Class0 • Class1 • Class2 • Class3 • Class4
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
Device class	Device type, which can be: • Connectivity device, indicating an intermediate device. • Class Ⅰ, indicating a normal terminal device. All terminal devices that are LLDP-enabled are of this type. • Class Ⅱ, indicating a media terminal device. A device of this type is media-capable. That is, besides the capabilities of a normal terminal device, it also supports media stream. • Class Ⅲ, indicating a communication terminal device. A device of this type supports IP communication systems of end user. A device of this type supports all the capabilities of a normal terminal device and a media terminal device and can be used directly by end users.
Media policy type	Media policy type, which can be: • unknown • voice • voiceSignaling • guestVoice • guestVoiceSignaling • softPhoneVoice • videoconferencing • streamingVideo • videoSignaling
Unknown Policy	Indicates whether or not the device can acquire media policy data
VLAN Tagged	Indicates whether packets of the media VLAN are tagged.
Media Policy VlanID	ID of the media VLAN
Media Policy L2 priority	Layer 2 priority
Media Policy Dscp	DSCP precedence
HardwareRev	Hardware version

Field	Description
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNumber	Serial number
Manufacturer name	Manufacturer name
Model name	Module name
Asset tracking identifier	Asset tracking ID
Location format	Location information format, which can be: • Invalid, indicating the format of the location information is invalid. • Coordinate-based LCI, indicating the location information is coordinate-based. • Civic Address LCI, indicating normal address information. • ECS ELIN, indicating a telephone for urgencies.
Location Information	Location information
PoE PSE power source	PSE type, which can be: • Primary, indicating a primary power supply • Backup, indicating a backup power supply
PoE service type	PoE service type
Port PSE Priority	Port PSE priority, which can be: • Unknown • Critical • High • Low
Available power value	PoE power
Unknown basic TLV	Unknown basic TLV
TLV type	Unknown basic TLV type
TLV information	Information contained in the unknown basic TLV type
Unknown organizationally-defined TLV	Unknown organization-defined TLV
TLV OUI	OUI of the unknown organization-defined TLV
TLV subtype	Unknown organization-defined TLV subtype
Index	Unknown organization index
TLV information	Information contained in unknown organization-defined TLV

display lldp statistics

Syntax

display lldp statistics [**global** | **interface** *interface-type interface-number*]

View

Any view

Parameters

global: Displays the global LLDP statistics.

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

Description

Use the **display lldp statistics** command to display the global LLDP statistics or the LLDP statistics of a port.

If no keyword/argument is specified, this command displays all the LLDP statistics.

Examples

Display all the LLDP statistics.

```
<Sysname> display lldp statistics
LLDP statistics global Information :
LLDP neighbor information last change time : 0 days, 0 hours, 4 minutes, 40 seconds
The number of neighbor information inserted  : 1
The number of neighbor information deleted   : 0
The number of neighbor information dropped   : 0
The number of 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 1-3 display lldp statistics command output description

Field	Description
lldp statistics global information	Global LLDP statistics
Neighbor information last change time	Time the neighbor information is latest updated
The number of neighbors inserted	Number of times of adding neighbor information
The number of neighbors deleted	Number of times of removing neighbor information
The number of neighbors dropped	Number of times of dropping neighbor information due to lack of available memory space
The number of neighbors aged out	Number of the neighbor information entries that have aged out
lldp statistics Information of port number *interface-type interface-number*	LLDP statistics of a port

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

display lldp status

Syntax

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

View

Any view

Parameters

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

Description

Use the **display lldp status** command to display the LLDP status of a port.

If no port is specified, this command displays the LLDP status of all the ports.

Examples

Display the LLDP status of all the ports.

```
<Sysname> display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 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
Roll time                       : 0s

Number of neighbors              : 5
Number of MED neighbors          : 2
Number of CDP neighbors          : 0
Number of sent optional TLV      : 12
Number of received unknown TLV   : 5
```

Table 1-4 display lldp status command output description

Field	Description
Global status of LLDP	Indicating whether or not LLDP is globally enabled
The current number of LLDP neighbors	Total number of the LLDP neighbor devices
The current number of CDP neighbors	The current number of CDP neighbors
Transmit interval	Interval to send LLDPDU
Hold multiplier	TTL multiplier
Reinit delay	Initialization delay
Transmit delay	Delay period to send LLDPDUs
Trap interval	Interval to send traps
Fast start times	Number of the LLDPDUs to be sent successively when a new neighboring device is detected
Port number *interface-type interface-number*	Port LLDP status
Port status of LLDP	Indicates whether or not LLDP is enabled on the port.
Admin status	LLDP mode of the port, which can be: • TxRx. A port in this mode sends and receives LLDPDUs. • Rx_Only. A port in this mode receives LLDPDUs only. • Tx_Only. A port in this mode sends LLDPDUs only. • Disable. A port in this mode does not send or receive LLDPDUs.
Trap Flag	Indicates whether or not trap is enabled.
Roll time	LLDP polling interval. A value of 0 indicates LLDP polling is disabled.
Number of neighbors	Number of the LLDP neighbors connecting to the port
Number of CDP neighbors	Number of the CDP neighbors connecting to the port

Field	Description
Number of sent optional TLV	Number of the optional TLVs contained in an LLDPDU sent through the port
Number of received unknown TLV	Number of the unknown TLVs contained in a received LLDPDU

display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*]

View

Any view

Parameters

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

Description

Use the **display lldp tlv-config** command to display the TLVs that are currently sent through a port.

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

Examples

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

```
<Sysname> display lldp tlv-config
LLDP tlv-config of port 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 1-5 display lldp tlv-config command output description

Field	Description
LLDP tlv-config of port number *interface-type interface-number*	TLVs that are currently sent through a port
NAME	TLV type
STATUS	Indicates whether or not TLVs of a specific type are currently sent through a port
DEFAULT	Indicates whether or not TLVs of a specific type are sent through a port by default
Basic optional TLV	Basic TLVs, including: • Port description TLV • System name TLV • System description TLV • System capabilities TLV • Management address TLV
IEEE 802.1 extended TLV	IEEE 802.1 extended TLVs, including: • Port VLAN ID TLV • Port and protocol VLAN ID TLV • VLAN name TLV
IEEE 802.3 extended TLV	IEEE 802.3 extended TLVs, including: • MAC-Physic TLV • Power via MDI TLV • Link aggregation TLV • Maximum frame size TLV
LLDP-MED extend TLV	MED related LLDP TLVs, including: • Capabilities TLV • Network Policy TLV • Extended Power-via-MDI TLV • Location Identification TLV • Inventory TLV, which can be hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV, and asset id TLV.

lldp admin-status

Syntax

lldp admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp admin-status

View

Ethernet interface view

Parameters

disable: Specifies the **Disable** mode. A port in this mode does not send or receive LLDPDUs.

rx: Specifies the **Rx** mode. A port in this mode receives LLDPDUs only.

tx: Specifies the **Tx** mode. A port in this mode sends LLDPDUs only.

txrx: Specifies the **TxRx** mode. A port in this mode sends and receives LLDPDUs.

Description

Use the **lldp admin-status** command to specify the LLDP operating mode for a port or all the ports in a port group.

Use the **undo lldp admin-status** command to restore the default LLDP operating mode.

The default LLDP operating mode is **TxRx**.

Examples

Configure the LLDP operating mode as **Rx** for GigabitEthernet 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 *value*

undo lldp check-change-interval

View

Ethernet interface view

Parameters

value: LLDP polling interval to be set, in the range 1 to 30 (in seconds).

Description

Use the **lldp check-change-interval** command to enable LLDP polling and set the polling interval.

Use the **undo lldp check-change-interval** command to restore the default.

By default, LLDP polling is disabled.

With LLDP polling enabled, LLDP detects for local configuration changes periodically. A local configuration change triggers LLDPDU sending, through which neighboring devices can be informed of the configuration change timely.

Examples

Enable LLDP polling on 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** }

View

Ethernet interface view

Parameters

disable: Specifies the disable mode, where CDP-compatible LLDP neither receives nor transmits CDP packets.

txrx: Specifies the TxRx mode, where CDP-compatible LLDP can send and receive CDP packets.

Description

Use the **lldp compliance admin-status cdp** command to configure the operation mode of CDP-compatible LLDP on a port or port group.

By default, CDP-compatible LLDP operates in disable mode.

To have your device work with Cisco IP phones, you must enable CDP-compatible LLDP globally and then configure CDP-compatible LLDP to work in TxRx mode on the specified port(s).

Examples

Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 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

Parameters

None

Description

Use the **lldp compliance cdp** command to enable global CDP compatibility.

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

By default, global CDP compatibility is disabled.

Note that, as the maximum TTL allowed by CDP is 255 seconds, your TTL configuration, that is, the product of the TTL multiplier and the LLDPDU sending interval, must be less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.

Related commands: **lldp hold-multiplier**, **lldp timer tx-interval**.

Examples

Enable LLDP to be compatible with CDP globally.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
```

lldp enable

Syntax

lldp enable

undo lldp enable

View

System view, Ethernet interface view

Parameters

None

Description

Use the **lldp enable** command to enable LLDP.

Use the **undo lldp enable** command to disable LLDP.

By default, LLDP is disabled globally, and is enabled on a port.

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

Examples

Disable LLDP on 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 [**snap**]

View

Ethernet interface view

Parameters

None

Description

Use the **lldp encapsulation snap** command to configure the encapsulation format for LLDPDUs as SNAP on a port or a group of ports.

Use the **undo lldp encapsulation** [**snap**] command to restore the default encapsulation format for LLDPDUs.

By default, Ethernet II encapsulation applies.

 **Note**

The command does not apply to LLDP-CDP packets, which use only SNAP encapsulation.

Examples

Configure the encapsulation format for LLDPDUs as SNAP on GigabitEthernet 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 *value*

undo lldp fast-count

View

System view

Parameters

value: Number of the LLDPDUs to be sent successively when a new neighboring device is detected. This argument ranges from 1 to 10.

Description

Use the **lldp fast-count** command to set the number of the LLDPDUs to be sent successively when a new neighboring device is detected.

Use the **undo lldp fast-count** command to restore the default.

By default, the number is 3.

Examples

Configure to send four LLDP successively when a new neighboring device is detected.

```
<Sysname> system-view
[Sysname] lldp fast-count 4
```

lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

View

System view

Parameters

value: TTL multiplier, in the range 2 to 10.

Description

Use the **lldp hold-multiplier** command to set the TTL multiplier.

Use the **undo lldp hold-multiplier command** to restore the default.

The TTL multiplier defaults to 4.

You can set the TTL of the local device information by configuring the TTL multiplier.

The TTL of the information about a device is determined by the following expression:

TTL multiplier × LLDPDU sending interval

You can set the TTL of the local device information by configuring the TTL multiplier. Note that the TTL can be up to 65535 seconds. TTLs longer than it will be rounded off to 65535 seconds.

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

Examples

Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

lldp management-address-tlv

Syntax

lldp management-address-tlv [*ip-address*]

undo lldp management-address-tlv

View

Ethernet interface view

Parameters

ip-address: Management address to be set.

Description

Use the **lldp management-address-tlv** command to enable the management address sending. This command also sets the management address.

Use the **undo lldp management-address-tlv** command to disable management address sending.

By default, the management address is sent through LLDPDUs, and the management address is the primary IP address of the VLAN with the least VLAN ID among the VLANs whose packets are permitted on the port. If the primary IP address is not configured, the management address is 127.0.0.1.

Note that an LLDPDU carries only one management address. If you set the management address repeatedly, the latest one takes effect.

Examples

Set the management address to 192.6.0.1 for 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

Ethernet interface view

Parameters

None

Description

Use the **lldp notification remote-change enable** command to enable trap for a port or all the ports in a port group.

Use the **undo lldp notification remote-change enable** command to restore the default.

By default, trap is disabled on a port.

Examples

Enable trap for 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 *value*

undo lldp timer notification-interval

View

System view

Parameters

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

Description

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

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

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

Examples

Set the interval to send trap messages to 8 seconds.

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

lldp timer reinit-delay

Syntax

lldp timer reinit-delay *value*

undo lldp timer reinit-delay

View

System view

Parameters

value: Initialization delay period to be set, in the range 1 to 10 (in seconds).

Description

Use the **lldp timer reinit-delay** command to set the initialization delay period.

Use the **undo lldp timer reinit-delay** command to restore the default.

By default, the initialization delay period is 2 seconds.

Examples

Set the initialization delay period to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer tx-delay

Syntax

lldp timer tx-delay *value*

undo lldp timer tx-delay

View

System view

Parameters

value: Delay period to send LLDPDUs, in the range 1 to 8192 (in seconds).

Description

Use the **lldp timer tx-delay** command to set the delay period to send LLDPDUs.

Use the **undo lldp timer tx-delay** command to restore the default.

By default, the delay period to send LLDPDUs is 2 seconds.

Examples

Set the delay period to send LLDPDUs to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-delay 4
```

lldp timer tx-interval

Syntax

lldp timer tx-interval *value*

undo lldp timer tx-interval

View

System view

Parameters

value: Interval to send LLDPDUs, in the range 5 to 32768 (in seconds).

Description

Use the **lldp timer tx-interval** command to set the interval to send LLDPDUs.

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

By default, the interval to send LLDPDUs is 30 seconds.

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

Examples

Set the interval to send LLDPDUs to 20 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

lldp tlv-enable

Syntax

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } | **network-policy** | **power-over-ethernet** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** | **network-policy** | **power-over-ethernet** } }

View

Ethernet interface view

Parameters

all: Sends all the basic LLDP TLVs, all the IEEE 802.1 defined LLDP TLVs, or all the IEEE 802.3 defined LLDP TLVs; or sends all the MED related LLDP TLVs except location identification TLVs.

basic-tlv: Sends basic LLDP TLVs.

port-description: Sends port description TLVs.

system-capability: Sends system capabilities TLVs.

system-description: Sends system description TLVs.

system-name: Sends system name TLVs.

dot1-tlv: Sends IEEE 802.1 defined LLDP TLVs.

port-vlan-id: Sends port VLAN ID TLVs.

protocol-vlan-id: Sends port and protocol VLAN ID TLVs.

vlan-name: Sends VLAN name TLVs.

vlan-id: ID of the VLAN the TLVs (port and protocol VLAN ID TLVs or VLAN name TLVs) concerning which are to be sent. This argument defaults to the least protocol VLAN ID.

dot3-tlv: Sends IEEE 802.3 defined LLDP TLVs.

link-aggregation: Sends link aggregation group TLVs.

mac-physic: Sends MAC/PHY configuration/status TLVs.

max-frame-size: Sends maximum frame size TLVS.

power: Sends power via MDI TLVs.

med-tlv: Sends MED related LLDP TLVs.

capability: Sends LLDP-MED capabilities TLVs.

inventory: Sends hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.

location-id: Sends location identification TLVS.

civic-address: Inserts the address information about the intermediate device in location identification TLVs .

device-type: Device type value. A value of 0 specifies DHCP server; a value of 1 specifies switch, and a value of 2 specifies LLDP-MED endpoint.

country-code: Country code, confirming to ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information, where *ca-type* represents the address information type, in the range 0 to 255, *ca-value* represents address information, a string of 1 to 250 characters, and &<1-10> indicates that you can enter up to ten such parameters.

elin-address: Inserts telephone numbers for urgencies in location identification TLVs.

tel-number: Telephone number for urgencies, a string of 10 to 25 characters.

network-policy: Sends network policy TLVs.

power-over-ethernet: Sends extended power-via-MDI TLVs.

Description

Use the **lldp tlv-enable** command to enable the sending of specific TLVs for a port or all the ports in a port group.

Use the **undo lldp tlv-enable** command to disable the sending of specific TLVs.

By default, all the TLVs except location identification TLVs are sent.

Note that:

- To enable MED related LLDP TLV sending, you need to enable LLDP-MED capabilities TLV sending first. Conversely, to disable LLDP-MED capabilities TLV sending, you need to disable the sending of other MED related LLDP TLV.
- To disable MAC/PHY configuration/status TLV sending, you need to disable LLDP-MED capabilities TLV sending first.
- Specifying the **all** keyword for basic LLDP TLVs and organization defined LLDP TLVs (including IEEE 802.1 defined LLDP TLVs and IEEE 802.3 defined LLDP TLVs) enables sending of all the corresponding LLDP TLVs. For MED related LLDP TLVs, the **all** keyword enables sending of all the MED related LLDP TLVs except location identification TLVs.
- Enabling the sending of LLDP-MED capabilities TLVs also enables the sending of MAC/PHY configuration/status TLVs.
- You can specify to send multiple types of TLVs by executing the **lldp tlv-enable** command repeatedly.

Examples

Enable the sending of link aggregation group TLVs on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

Table of Contents

1 Access Management Configuration Commands

Access Management Configuration Commands

am enable

Syntax

am enable

undo am enable

View

System view

Parameters

None

Description

Use the **am enable** command to enable the access management function.

Use the **undo am enable** command to disable the function.

By default, Access management function is disabled.

Before enabling access management, you are recommended to cancel the static ARP configuration to ensure that the binding of IP address and Ethernet switch can take effect.

Examples

Enable the access management function.

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

am ip-pool

Syntax

am ip-pool *address-list*

undo am ip-pool { **all** | *address-list* }

View

Ethernet port view

Parameters

all: Specifies all the IP addresses (or IP address pools).

address-list: IP address list. You need to provide this argument in the format of *start-ip-address* [*ip-address-number*] & < 1-10 >, where *start-ip-address* is the start IP address of an IP address range in the address pool, *ip-address-number* specifies the number of the successive IP addresses following *start-ip-address* in the range, and & < 1-10 > means you can specify up to ten IP addresses/IP address ranges.

Description

Use the **am ip-pool** command to configure the access management IP address pool on a port. For a port with the access management IP address pool configured, only the hosts with their IP addresses being in the access management pool can access external networks through the port.

Use the **undo am ip-pool** command to remove part of or all the IP addresses from the access management IP address pool of a port.

By default, the access management IP address pool is null.

Note that:

- Before configuring the access management IP address pool of a port, you need to configure the interface IP address of the VLAN to which the port belongs, and the IP addresses in the access management IP address pool of a port must be in the same network segment as the interface IP address of the VLAN which the port belongs to.
- If an access management address pool configured contains IP addresses that belong to the static ARP entries of other ports, the system prompts you to delete the corresponding static ARP entries to ensure the access management IP address pool can take effect.

Examples

Configure the access management IP address pool on GigabitEthernet 1/0/1 to allow hosts with their IP addresses being in the range 202.112.66.2 to 202.112.66.20 and 202.112.65.1 to access external networks through the port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] am ip-pool 202.112.66.2 19 202.112.65.1
```

Remove all the IP addresses from the access management IP address pool of port GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] undo am ip-pool all
```

am trap enable

Syntax

am trap enable

undo am trap enable

View

System view

Parameters

None

Description

Use the **am trap enable** command to enable the access management trap function.

Use the **undo am trap enable** command to disable the access management trap function.

By default, the access management trap function is disabled.

Examples

Enable the access management trap.

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

display am

Syntax

display am [*interface-list*]

View

Any view

Parameters

interface-list: Port list. You need to provide this argument in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where *interface-type* is port type, *interface-number* is port number, and &<1-10> means that you can specify up to ten ports/port lists.

Description

Use the **display am** command to display the current access management configuration, including the status (enabled/disabled), and the access management IP address pool configuration information.

If you do not specify the *interface-list* argument, this command displays the current access management configuration of all the ports.

Examples

Display the access management configurations of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> display am GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
GigabitEthernet1/0/1
 Status       : enabled
 IP Pools     : 10.10.1.1(19) 10.10.1.30(1)
GigabitEthernet1/0/2
 Status       : enabled
 IP Pools     : (NULL)
```

Table 1-1 Description on the fields of the **display am** command

Field	Description
Status	Access Management state of a port: enabled or disabled

Field	Description
IP Pools	Access management IP pools. NULL means the access management IP pool is not configured. Each IP address range is represented as X.X.X.X (number), among which “X.X.X.X” is the starting address and “number” indicates the number of successive IP addresses contained in the IP address range.

Table of Contents

1 UDP Helper Configuration Commands

UDP Helper Configuration Commands

display udp-helper server

Syntax

display udp-helper server [**interface Vlan-interface** *vlan-id*]

View

Any view

Parameters

vlan-id: VLAN interface number.

Description

Use the **display udp-helper server** command to display the UDP broadcast relay forwarding information. The information includes the VLAN interface enabled with UDP Helper, IP address of the destination server, and the number of UDP packets forwarded to the destination server. If a *vlan-id* is specified, UDP broadcast relay forwarding information of the specified VLAN interface is displayed.

Examples

Display the UDP broadcast relay forwarding information on VLAN-interface 1.

```
<Sysname> display udp-helper server interface Vlan-interface 1
 Interface name        Server address       Packets sent
 Vlan-interface1       192.1.1.2            0
```

The information above shows that the IP address of the destination server corresponding to VLAN-interface 1 is 192.1.1.2, and no packets have been forwarded to the destination server.

Table 1-1 Description on the fields of the **display udp-helper server** command

Field	Description
Interface name	Interface enabled with UDP Helper
Server address	Destination server IP address to which UDP packets are forwarded
Packets sent	Number of UDP packets forwarded to the destination server

reset udp-helper packet

Syntax

reset udp-helper packet

View

User view

Parameters

None

Description

Use the **reset udp-helper packet** command to clear UDP Helper statistics.

Examples

Clear UDP Helper statistics.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

View

System view

Parameters

None

Description

Use the **udp-helper enable** command to enable UDP Helper function. After this function is enabled, the switch converts broadcasts containing the specified port numbers into unicasts and forwards them to the destination server.

Use the **undo udp-helper enable** command to disable UDP Helper function.

By default, UDP Helper is disabled.

Examples

Enable UDP Helper.

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

Parameters

port-number: Number of the UDP port with which UDP packets are to be forwarded, in the range 0 to 65535 (except for 67 and 68).

dns: Forwards Domain Name System (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 Trivial File Transfer Protocol (TFTP) data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description

Use the **udp-helper port** command to configure the UDP port with which broadcast packets are to be forwarded.

Use the **undo udp-helper port** command to remove the configuration.

By default, the UDP Helper enabled device forwards broadcast packets with any of the six UDP port numbers 53, 138, 137, 49, 69 and 37.

Note that:

- You need to enable the UDP Helper function before specifying any UDP port; otherwise, the system prompts error information. When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.
- The relaying of BOOTP/DHCP broadcast packets is implemented through the DHCP relay agent function using UDP port 67 and 68. That is, the UDP port number cannot be set to 67 or 68 for UDP Helper.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords correspond to the six default ports. You can configure the default ports by specifying port numbers or the corresponding parameters. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same port.
- When you view the configuration information by using the **display current-configuration** command, information about default UDP ports is not displayed. Such information is displayed only when a default port is disabled.
- Currently, you can configure up to 256 UDP ports on the device.

Examples

Enable forwarding of UDP broadcasts with a destination UDP port number of 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] udp-helper port 100
```

Disable forwarding of UDP broadcasts with a destination UDP port number of 53.

```
[Sysname] undo udp-helper port 53
```

udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

VLAN interface view

Parameters

ip-address: IP address of the destination server, in dotted decimal notation.

Description

Use the **udp-helper server** command to specify the destination server to which the UDP packets are to be forwarded.

Use the **undo udp-helper server** command to remove the specified destination server.

No destination server is specified by default.

Note that:

- Executing the **undo udp-helper server** command without specifying the *ip-address* argument removes all the destination servers configured on the current interface.
- You can specify up to 20 destination server IP addresses on a VLAN interface.

Related commands: **display udp-helper server**.

Examples

Specify the destination server at 192.1.1.2 for VLAN-interface 1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] udp-helper server 192.1.1.2
```

Remove all the specified destination servers for VLAN-interface 1.

```
[Sysname-Vlan-interface1] undo udp-helper server
```

udp-helper ttl-keep enable

Syntax

udp-helper ttl-keep enable

undo udp-helper ttl-keep enable

View

System view

Parameters

None

Description

Use the **udp-helper ttl-keep enable** command to enable the UDP Helper TTL-keep function. With this function enabled, the UDP Helper can forward broadcasts with the TTL field being 1 without decrementing the TTL value by one.

Use the **undo udp-helper ttl-keep enable** command to restore the default.

By default, the UDP Helper TTL-keep function is disabled.

Note that you need to enable UDP Helper before enabling the TTL-keep function; otherwise, the TTL-keep function does not take effect.

Examples

Enable the UDP Helper TTL-keep function on the switch.

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